

(11)特許出願公開番号

**特開2004-112788**

(P2004-112788A)

(43) 公開日 平成16年4月8日(2004.4.8)

(51) Int. Cl.<sup>7</sup>

H04L 9/08

HO4L 9/32

F1

HO4 L 9/00 601 B

HO4 L 9/00 601 E

HO 4 L 9/00 6 7 5 B

テーマコード (参考)

5 J 104

審査請求 未請求 請求項の数 24 O L (全 94 頁)

(21) 出願番号 特願2003-305399 (P2003-305399)

(22) 出題日 平成15年8月28日 (2003. 8. 28)

(31) 優先權主張番号 特願2002-249242 (P2002-249242)

(32) 優先日 平成14年8月28日 (2002. 8. 28)

(33) 優先権主張国 日本国 (JP)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(74) 代理人 100090446

弁理士 中島 司朗

(72) 発明者 太田 雄策

大阪府門真市大字門真1006番地 松下  
電器産業株式会社内

(72) 発明者 山内 弘貴

大阪府門真市大字門真1006番地 松下  
電器産業株式会社内

(72) 発明者 宮▲さき▼ 雅也

大阪府門真市大字門真1006番地 松下  
電器産業株式会社内

[最終頁に続く](#)

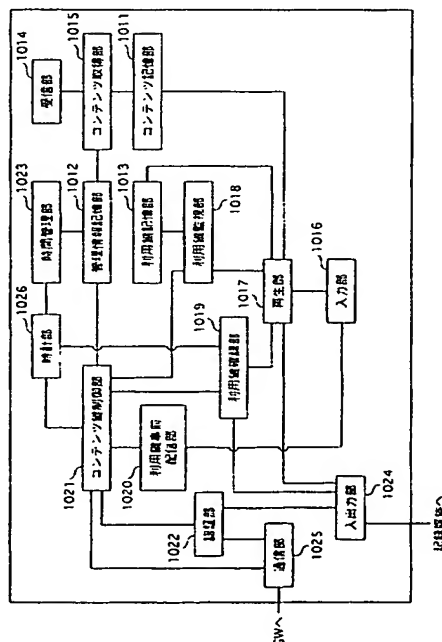
(54) 【発明の名称】 鍵配信装置、端末装置、記録媒体及び鍵配信システム

(57) 【要約】

【課題】 コンテンツが不正に使用されることを防止する鍵配信装置を提供することを目的とする。

【解決手段】 ネットワークに接続する１以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、前記端末装置から前記復号鍵の供給の要求を受け付け、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第１タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第２タイプの端末装置であるかの判断を行い、供給先が前記第１のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第２のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する。

【選択図】 図17



**BEST AVAILABLE COPY**

## 【特許請求の範囲】

## 【請求項 1】

ネットワークに接続する 1 以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、

供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第 1 タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第 2 タイプの端末装置であるかの判断を行う供給判断手段と、

供給先が前記第 1 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第 2 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、

前記供給判断手段は、少なくとも、可搬型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第 1 のタイプと判断する

ことを特徴とする鍵配信装置。

## 【請求項 2】

前記ネットワークは、外部ネットワークに接続するホームネットワークであり、前記コンテンツは、前記ホームネットワーク外から受信され、前記鍵配信装置は、少なくともホームネットワークに接続される端末装置を、前記復号鍵の正当な供給先と判断する

ことを特徴とする請求項 1 に記載の鍵配信装置。

## 【請求項 3】

前記鍵配信装置は、さらに、

前記第 1 のタイプの端末装置へ前記復号鍵と前記利用期限とを供給後、前記利用期限を記憶する配信鍵情報記憶手段と、

前記配信鍵情報記憶手段に記憶している前記利用期限が切れているか否かの判断を行う期限判断手段と、

前記利用期限が切れていると判断する場合には、前記管理数に 1 加算する時間管理手段と

を備えることを特徴とする請求項 1 に記載の鍵配信装置。

## 【請求項 4】

前記鍵配信装置は、さらに、

前記復号鍵と前記利用期限とを供給すべき日時を示す供給日時と、供給先が第 1 のタイプの端末装置であることを示す識別情報とからなる組、又は前記復号鍵を供給すべき日時を示す供給日時と、供給先が第 2 のタイプの端末装置であることを示す識別情報とからなる組のうち少なくともどちらかを記憶する日時記憶手段と、

現在の日時が、前記供給日時記憶手段にて記憶されている供給日時に到達したか否かを判断する日時判断手段と、

前記日時判断手段が供給日時に到達したと判断する場合、前記識別情報に基づいて、前記復号鍵と前記利用期限とを前記第 1 のタイプの端末装置へ供給、又は前記復号鍵を前記第 2 のタイプの端末装置へ供給する日時供給手段と

を備えることを特徴とする請求項 3 に記載の鍵配信装置。

## 【請求項 5】

前記鍵配信装置は、さらに、

前記復号鍵を示す検索情報を前記第 1 タイプの端末装置及び前記第 2 のタイプの端末装置へ通知する検索要求手段と、

前記第 1 のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第 1 のタイプの端末装置より受け取り、前記第 2 のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第 2 のタイプの端末装置より受け取る所有情報受取手段と

を備えることを特徴とする請求項 4 に記載の鍵配信装置。

## 【請求項 6】

前記鍵配信装置は、供給先が正当な供給先であるか否かの基準となる秘密情報を記憶しており、

前記供給判断手段は、供給先が、前記秘密情報を所有しているか否かの判断を行うサーバ認証手段を含み、

前記供給判断手段は、サーバ認証手段にて供給先が前記秘密情報を所有していると判断する場合に、正当な供給先と判断する

ことを特徴とする請求項 5 に記載の鍵配信装置。

## 【請求項 7】

前記鍵配信手段は、前記復号鍵の管理数が、予め定められた基準値より大きいと判断する残数判断手段を含み、 10

前記鍵配信手段は、前記残数判断手段にて、前記管理数が、前記基準値より大きいと判断する場合に、残数があると判断する

ことを特徴とする請求項 6 に記載の鍵配信装置。

## 【請求項 8】

前記鍵供給手段は、さらに、

前記第 1 のタイプの端末装置へ前記復号鍵と前記利用期限とを供給する場合には、前記復号鍵と前記利用期限とを暗号化し、前記第 2 のタイプの端末装置へ前記復号鍵を供給する場合には、前記復号鍵を暗号化する暗号処理手段を備え、

前記鍵供給手段は、供給先が前記第 1 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを、前記暗号処理手段にて暗号化して、前記端末装置へ供給し、供給先が前記第 2 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を、前記暗号処理手段にて暗号化して、前記端末装置へ供給する 20

ことを特徴とする請求項 7 に記載の鍵配信装置。

## 【請求項 9】

前記鍵配信装置は、さらに、

前記第 1 のタイプの端末装置が接続された日時を示す履歴情報を記憶する履歴情報記憶手段と、

前記履歴情報を用いて、前記第 1 のタイプの端末装置が予め設定された接続期間内に接続がなされたか否かの判断を行う接続判断手段と、 30

前記接続期間内に接続がされていないと判断する場合には、前記管理数に 1 加算する接続管理手段とを

備えることを特徴とする請求項 8 に記載の鍵配信装置。

## 【請求項 10】

前記鍵配信装置は、さらに、

前記第 1 のタイプの端末装置が前記復号鍵を利用した回数を記憶する回数記憶手段と、

前記回数が、予め設定された利用回数に達したか否かの判断を行う回数判断手段と、

前記利用回数に達したと判断する場合には、前記管理数に 1 加算する接続管理手段とを 40

備えることを特徴とする請求項 8 に記載の鍵配信装置。

## 【請求項 11】

暗号化鍵にて暗号化されたコンテンツを復号する復号鍵を管理する鍵配信装置よりネットワークを介して前記復号鍵の供給を受ける端末装置であって、

前記鍵配信装置へ前記復号鍵を要求する要求手段と、

前記鍵配信装置にて前記復号鍵が供給可能であると判断される場合に、前記復号鍵を、前記鍵配信装置より受け取る鍵受付手段と、

受け取った前記復号鍵を用いて、前記コンテンツの利用が終了したことを検知する検知手段と、

前記検知手段にて前記コンテンツの利用が終了したことを検知した場合に、前記復号鍵を消去し、前記復号鍵の利用が終了したことを示す利用終了情報を前記鍵配信装置へ通知 50

する終了通知手段と

を備えることを特徴とする端末装置。

【請求項 12】

前記端末装置は、さらに、

前記鍵受付手段にて受け取った復号鍵を用いて、前記暗号化されたコンテンツを復号して、コンテンツを生成し、生成したコンテンツを利用する利用手段を備え、

前記検知手段は、前記利用手段による前記コンテンツの利用終了が終了したことを検知する

ことを特徴とする請求項 11 に記載の端末装置。

【請求項 13】

前記鍵受付手段は、さらに、

前記鍵配信装置より前記復号鍵を受け取る場合に、暗号化された復号鍵を受け取り、受け取った暗号化された復号鍵を復号して、前記復号鍵を生成する復号処理手段を備えることを特徴とする請求項 12 に記載の端末装置。

【請求項 14】

前記端末装置は、コンテンツの利用期限の管理を行う端末装置であって、

前記鍵受付手段は、さらに、前記復号鍵の利用期限を受け取り、

前記端末装置は、さらに、前記鍵受付手段にて受け取った前記期間情報にて示される前記利用期限が期限内であるか否かの判断を行う期限判断手段を備え、

前記検知手段は、前記期限判断手段にて、前記復号鍵の利用期限が過ぎたと判断する場合に、前記コンテンツの利用が終了したと検知する

ことを特徴とする請求項 11 に記載の端末装置。

【請求項 15】

前記鍵受付手段は、さらに、

前記鍵配信装置より前記復号鍵と前記利用期限を受け取る場合に、暗号化された復号鍵と利用期限とを受け取り、受け取った暗号化された復号鍵と利用期限とを復号して、前記復号鍵と前記利用期限とを生成する復号処理手段を

備えることを特徴とする請求項 12 に記載の端末装置。

【請求項 16】

前記端末装置は、さらに、

前記鍵配信装置より前記復号鍵を示す検索情報を受け取り、受け取った前記検索情報を用いて、前記復号鍵を所有しているか否かの判断を行う所有判断手段と、

前記所有判断手段にて、前記復号鍵を所有していると判断する場合には、前記復号鍵を所有する旨の情報を、前記鍵配信装置へ通知する所有通知手段と

を備えることを特徴とする請求項 11 に記載の端末装置。

【請求項 17】

暗号化鍵にて暗号化されたコンテンツを復号する復号鍵を管理する鍵配信装置より前記復号鍵の供給を受ける可搬型の記録媒体であって、

前記鍵配信装置にて前記復号鍵が供給可であると判断される場合に、前記復号鍵と前記復号鍵の利用期限とを、前記鍵配信装置より受け取る鍵受付手段と、

受け取った前記復号鍵と前記利用期限とを記憶する鍵情報記憶手段と

を備えることを特徴とする記録媒体。

【請求項 18】

前記鍵受付手段は、さらに、

前記鍵配信装置より前記復号鍵と前記利用期限を受け取る場合に、暗号化された復号鍵と利用期限とを受け取り、受け取った暗号化された復号鍵と利用期限とを復号して、前記復号鍵と前記利用期限とを生成する復号処理手段を

備えることを特徴とする請求項 17 に記載の記録媒体。

【請求項 19】

前記記録媒体は、さらに、

10

20

30

40

50



前記利用期限が切れているか否かの判断を行う期限判断手段と、

期限判断手段にて利用期限が切れていると判断する場合に、前記復号鍵と利用期限とを消去する消去手段と

を備えることを特徴とする請求項 17 に記載の記録媒体。

【請求項 20】

前記記録媒体は、さらに、

前記鍵配信装置より、前記復号鍵を示す鍵検索情報を受け取り、受け取った前記鍵検索情報を用いて、前記復号鍵を所有しているか否かの判断を行う所有判断手段と、

前記所有判断手段にて、前記復号鍵を所有していると判断する場合には、前記復号鍵を所有する旨の情報を、前記鍵配信装置へ通知する所有通知手段と

を備えることを特徴とする請求項 17 に記載の記録媒体。

【請求項 21】

ネットワークに接続する 1 以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置と、コンテンツの利用期限の管理を行う第 1 タイプの端末装置と、コンテンツの利用期限の管理を行わない第 2 タイプの端末装置とからなる鍵配信システムであって、

前記鍵配信装置は、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第 1 タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第 2 タイプの端末装置であるかの判断を行う供給判断手段と、供給先が前記第 1 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第 2 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、前記供給判断手段は、少なくとも、可搬型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第 1 のタイプと判断し、

前記第 1 のタイプの端末装置は、

前記鍵配信装置より前記復号鍵と前記利用期限とを受け取り、受け取った前記復号鍵と前記利用期限とを記憶し、

前記第 2 のタイプの端末装置は、

前記鍵配信装置より前記復号鍵を受け取り、受け取った前記復号鍵を用いて、コンテンツを利用する

ことを特徴とする鍵配信システム。

【請求項 22】

ネットワークに接続する 1 以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置に用いられる鍵供給方法であって、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付ステップと、

供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第 1 タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第 2 タイプの端末装置であるかの判断を行う供給判断ステップと、

供給先が前記第 1 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第 2 のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給ステップと

を含むことを特徴とする鍵供給方法。

【請求項 23】

ネットワークに接続する 1 以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置に用いられる鍵供給プログラムであって、

10

20

30

40

50

前記端末装置から前記復号鍵の供給の要求を受け付ける受付ステップと、

供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第1タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第2タイプの端末装置であるかの判断を行う供給判断ステップと、

供給先が前記第1のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第2のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給ステップと

を含むことを特徴とする鍵供給プログラム。

【請求項24】

ネットワークに接続する1以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置に用いられる鍵供給プログラムを記録しているコンピュータ読み取り可能なプログラム記録媒体であって、

前記鍵供給プログラムは、

前記端末装置から前記復号鍵の供給の要求を受け付ける受付ステップと、

供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第1タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第2タイプの端末装置であるかの判断を行う供給判断ステップと、

供給先が前記第1のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第2のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給ステップと

を含むことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、暗号化されたコンテンツを復号する鍵を配信する技術に関する。

【背景技術】

【0002】

近年、映画、音楽、ゲームプログラム等のデジタル化されたコンテンツにおける著作権の保護が求められており、コンテンツの管理が重要となってきた。

特許文献1において、複製コンテンツの数を規制して著作権の保護を図るコンテンツ管理に有効な技術が開示されている。この方法では、記録媒体に記録する複製コンテンツの数を規制しながら該記録媒体に複製コンテンツを記録する記録装置と、該記録媒体との間の相互認証を行い、該記録装置は、認証が成功すると該記録媒体へ複製コンテンツを複製若しくは、削除することによりコンテンツ利用の管理を行っている。

【特許文献1】特開2000-357213号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

しかしながら、上記に示した方法では、記録装置は、ネットワークに接続された装置に記録された複製コンテンツ利用の管理を常に行うことはできるが、記録媒体に記録された複製コンテンツ利用の管理を行うことができるのは、前記記録媒体と接続された場合のみである。そのため、例えば、前記記録媒体が、第三者によって、前記記録媒体に記録されている複製コンテンツが不正に使用される可能性がある。

【0004】

そこで、本発明では、上記問題点を解決するために、コンテンツが不正に使用されることを防止する鍵配信装置、端末装置、記録媒体、鍵配信システム、鍵配信方法、プログラムを提供することを目的とする。

【課題を解決するための手段】

10

20

30

40

50

## 【0005】

上記目的を達成するために、本発明は、ネットワークに接続する1以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第1タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第2タイプの端末装置であるかの判断を行う供給判断手段と、供給先が前記第1のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第2のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、前記供給判断手段は、少なくとも、可機型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第1のタイプと判断することを特徴とする。

10

## 【発明の効果】

## 【0006】

本発明は、ネットワークに接続する1以上の端末装置に対し、暗号化されたコンテンツを復号する復号鍵と、前記復号鍵の供給可能な管理数とを管理する鍵配信装置であって、前記端末装置から前記復号鍵の供給の要求を受け付ける受付手段と、供給先が、正当な供給先であれば、その種類がコンテンツの利用期限の管理を行う第1タイプの端末装置であるか、コンテンツの利用期限の管理を行わない第2タイプの端末装置であるかの判断を行う供給判断手段と、供給先が前記第1のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを前記端末装置へ供給し、供給先が前記第2のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を前記端末装置へ供給する鍵供給手段とを備え、前記供給判断手段は、少なくとも、可機型の記録媒体に暗号化されたコンテンツと、前記復号鍵と、前記利用期限とを記録する端末装置を第1のタイプと判断することを特徴とする。

20

## 【0007】

この構成によると、鍵配信装置は、復号鍵の供給先が正当な供給先であれば、供給先が、第1のタイプの端末装置であるか又は第2のタイプの端末装置であるかの判断を行い、供給先が第1のタイプの端末装置である場合には、利用期限を付加した復号鍵を供給し、供給先が第2のタイプの端末装置である場合には、復号鍵を供給する。これにより、第1のタイプの端末装置には、利用期限を付加した復号鍵が供給されるため、第1のタイプの端末装置は、供給された利用期限と復号鍵とを使用することにより、コンテンツ利用の管理が可能となり、コンテンツの不正使用を防止することができる。

30

## 【0008】

ここで、前記ネットワークは、外部ネットワークに接続するホームネットワークであり、前記コンテンツは、前記ホームネットワーク外から受信され、前記鍵配信装置は、少なくともホームネットワークに接続される端末装置を、前記復号鍵の正当な供給先と判断するとしてもよい。

この構成によると、鍵配信装置は、ホームネットワークに接続される端末装置を正当な供給先と判断し、復号鍵を供給することができる。

40

## 【0009】

ここで、前記鍵配信装置は、さらに、前記第1のタイプの端末装置へ前記復号鍵と前記利用期限とを供給後、前記利用期限を記憶する配信鍵情報記憶手段と、前記配信鍵情報記憶手段に記憶している前記利用期限が切れているか否かの判断を行う期限判断手段と、前記利用期限が切れていると判断する場合には、前記管理数に1加算する時間管理手段とを備えるとしてもよい。

## 【0010】

この構成によると、前記第1のタイプの端末装置へ供給した復号鍵の利用期限を管理することにより、管理数の管理ができる。

50

ここで、前記鍵配信装置は、さらに、前記復号鍵と前記利用期限とを供給すべき日時を示す供給日時と、供給先が第1のタイプの端末装置であることを示す識別情報とからなる組、又は前記復号鍵を供給すべき日時を示す供給日時と、供給先が第2のタイプの端末装置であることを示す識別情報とからなる組のうち少なくともどちらかを記憶する日時記憶手段と、現在の日時が、前記供給日時記憶手段にて記憶されている供給日時に到達したか否かを判断する日時判断手段と、前記日時判断手段が供給日時に到達したと判断する場合、前記識別情報に基づいて、前記復号鍵と前記利用期限とを前記第1のタイプの端末装置へ供給、又は前記復号鍵を前記第2のタイプの端末装置へ供給する日時供給手段とを備えるとしてもよい。

#### 【0011】

この構成によると、供給日時記憶手段にて記憶されている供給日時となった場合に、復号鍵の供給を行うことができる。

ここで、前記鍵配信装置は、さらに、前記復号鍵を示す検索情報を前記第1タイプの端末装置及び前記第2のタイプの端末装置へ通知する検索要求手段と、前記第1のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第1のタイプの端末装置より受け取り、前記第2のタイプの端末装置が前記復号鍵を所有している場合に、前記復号鍵を所有する旨の情報を前記第2のタイプの端末装置より受け取る所有情報受取手段とを備えるとしてもよい。

#### 【0012】

この構成によると、鍵配信装置は、鍵検索情報を第1のタイプの端末装置及び第2のタイプの端末装置へ送信し、復号鍵を所有する旨の情報を受信することにより、復号鍵の供給先を検索することができる。

ここで、前記鍵配信装置は、供給先が正当な供給先であるか否かの基準となる秘密情報を記憶しており、前記供給判断手段は、供給先が、前記秘密情報を所有しているか否かの判断を行うサーバ認証手段を含み、前記供給判断手段は、サーバ認証手段にて供給先が前記秘密情報を所有していると判断する場合に、正当な供給先と判断するとしてもよい。

#### 【0013】

この構成によると、秘密情報を用いて、正当な供給先であるか否かの判断が可能となる。

ここで、前記鍵配信手段は、前記復号鍵の管理数が、予め定められた基準値より大きい  
か否かを判断する残数判断手段を含み、前記鍵配信手段は、前記残数判断手段にて、前記  
管理数が、前記基準値より大きいと判断する場合に、残数があると判断するとしてもよい

#### 【0014】

この構成によると、管理数と基準値とを用いて、残数の有無の判断を行うことが可能となる。

ここで、前記鍵供給手段は、さらに、前記第1のタイプの端末装置へ前記復号鍵と前記利用期限とを供給する場合には、前記復号鍵と前記利用期限とを暗号化し、前記第2のタイプの端末装置へ前記復号鍵を供給する場合には、前記復号鍵を暗号化する暗号処理手段を備え、前記鍵供給手段は、供給先が前記第1のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵と前記復号鍵に対応する利用期限とを、前記暗号処理手段にて暗号化して、前記端末装置へ供給し、供給先が前記第2のタイプの端末装置であると判断する場合、前記管理数の残数があれば、前記復号鍵を、前記暗号処理手段にて暗号化して、前記端末装置へ供給するとしてもよい。

#### 【0015】

この構成によると、復号鍵を供給する場合に暗号化することにより、安全に復号鍵の供給ができる。

ここで、前記鍵配信装置は、さらに、前記第1のタイプの端末装置が接続された日時を示す履歴情報を記憶する履歴情報記憶手段と、前記履歴情報を用いて、前記第1のタイプの端末装置が予め設定された接続期間内に接続がなされたか否かの判断を行う接続判断手

10

20

30

40

50

段と、前記接続期間内に接続がされていないと判断する場合には、前記管理数に1加算する接続管理手段とを備えるとしてもよい。

#### 【0016】

この構成によると、復号鍵を記憶している第1のタイプの端末装置が、予め設定された期間内に鍵配信装置と接続がなされたか否かを判断することにより、管理数の管理が可能となる。

ここで、前記鍵配信装置は、さらに、前記第1のタイプの端末装置が前記復号鍵を利用した回数を記憶する回数記憶手段と、前記回数が、予め設定された利用回数に達したか否かの判断を行う回数判断手段と、前記利用回数に達したと判断する場合には、前記管理数に1加算する接続管理手段とを備えるとしてもよい。

#### 【0017】

この構成によると、第1のタイプの端末装置へ供給した復号鍵を利用した回数が、予め記憶している利用回数に達したか否かを判断することにより、管理数の管理が可能となる。

また、本発明は、暗号化鍵にて暗号化されたコンテンツを復号する復号鍵を管理する鍵配信装置より前記復号鍵の供給を受ける可搬型の記録媒体であって、前記鍵配信装置にて前記復号鍵が供給可能であると判断される場合に、前記復号鍵と前記復号鍵の利用期限とを、前記鍵配信装置より受け取る鍵受付手段と、受け取った前記復号鍵と前記利用期限とを記憶する鍵情報記憶手段とを備える。

#### 【0018】

この構成によると、記録媒体は、受け取った期限付復号鍵を用いて、復号鍵と利用期限とを生成し、生成した復号鍵と利用期限とを記憶することができる。

ここで、前記記録媒体は、さらに、前記利用期限が切れているか否かの判断を行う期限判断手段と、期限判断手段にて利用期限が切れていると判断する場合には、前記復号鍵と利用期限とを消去する消去手段とを備えるとしてもよい。

#### 【0019】

この構成によると、前記利用期限が過ぎている場合には、記憶している復号鍵と利用期限とを消去する。これにより、利用期限が過ぎている復号鍵の利用を防止することができる。

#### 【発明を実施するための最良の形態】

#### 【0020】

以下、本発明の実施の形態について図面を用いて詳細に説明する。

#### 1. グループ形成管理システム1の構成

グループ形成管理システム1は図1に示すように、AD内サーバ100、再生装置200、車載機器300、ICカード400及びDVD500から構成される。

AD内サーバ100及びモニタ251とスピーカ252とが接続されている再生装置200は、ユーザ宅内に設置されており、オンラインで接続されている。車載機器300は、ユーザが所有する車両に搭載されている。ICカード400及びDVD500は、AD内サーバ100及び車載機器300に接続可能である。ICカード400はAD内サーバ100に付属しており、AD内サーバ100は、ICカード400が接続されている場合のみ、動作する。

#### 【0021】

グループ形成管理システム1は、AD内サーバ100が、コンテンツの利用が許可される範囲であるAD(AuthORIZED Domain)を管理するシステムである。

AD内サーバ100は、クライアント機器の登録を受け付けて管理し、AD内サーバ100及び登録されたクライアント機器は、AD内サーバ100により生成された共通秘密情報(以下CSI: Common Secret Information)を共有する。同一AD内の機器間では、共有したCSIを用いてお互いを認証し、認証に成功した場合にコンテンツの送受信やコピーを行う。前記CSIを持たない機器は、コンテンツの送受信やコピーを行うことは出来ない。

10

20

30

40

50

## 【0022】

再生装置200は、AD内サーバ100と接続されているので、認証を行い、クライアント機器として登録することが出来る。また、車載機器300は、AD内サーバ100と接続されていないが、ICカード400にCSIを記憶させ、ICカード400から車載機器300にCSIを通知することによってクライアント機器として登録することが出来る。

## 1. 1 AD内サーバ100の構成

AD内サーバ100は図2に示すように、制御部101、秘密鍵格納部102、公開鍵証明書格納部103、CRL格納部104、公開鍵暗号処理部105、登録情報記憶部106、CSI生成部107、CSI格納部108、コンテンツ格納部109、暗号化部110、ID格納部111、ドライブ部112、入力部113、表示部114、入出力部115、入出力部116、復号部117及び暗号化部119から構成される。

## 【0023】

AD内サーバ100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニットなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、AD内サーバ100は、その機能を達成する。

## 【0024】

AD内サーバ100は、機器の登録、CSIの移動及び脱退の管理、コンテンツの配送及びコンテンツのコピーの処理を行う。

以下、各構成について説明する。

## (1) 入出力部115、116、ドライブ部112

入出力部115は、再生装置200とデータの送受信を行う。入出力部116は、ICカード400が接続されたことを検出すると、制御部101に検出を出力する。また、ICカード400とデータの送受信を行う。ドライブ部112は、DVD500へデータの書き込み、読み出しを行う。

## (2) 秘密鍵格納部102、公開鍵証明書格納部103、CRL格納部104、コンテンツ格納部109、ID格納部111、コンテンツ鍵格納部118

ID格納部111は、AD内サーバ100に固有のIDであるID-1を記憶している

## 【0025】

公開鍵証明書格納部103は、公開鍵証明書Cert-1を格納する。

公開鍵証明書Cert-1は、公開鍵PK-1がAD内サーバ100の正しい公開鍵であることを証明するものである。公開鍵証明書Cert-1は、署名データSig-CA1、公開鍵PK-1及びID-1を含む。署名データSig-CA1は、CA(Certificate Authority)により、AD内サーバ100の公開鍵PK-1及びID-1に対して署名アルゴリズムSを施して生成した署名データである。ここでCAとは、信頼できる第三者機関であり、グループ形成管理システム1に属する機器の公開鍵の正当性を証明する公開鍵証明書を発行する機関である。なお、署名アルゴリズムSは、一例として、有限体上のElGamal署名である。ElGamal署名については、公知であるので説明を省略する。

## 【0026】

秘密鍵格納部102は、外部から内部を見ることが出来ない耐タンパ領域であり、公開鍵PK-1に対応する秘密鍵SK-1を格納する。

CRL格納部104は、CRL(Certificate Revocation List)を格納する。このCRLは、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器のIDが登録されたリストであり、CAから発行される。なお、CRLに登録されるのは、機器のIDでなくてもよく、無効化された機器が有する公開鍵証明書のシリアル番号が登録されるとしても良い。CRLは、放送、インターネット又は

DVD等の記録媒体に記録されて各機器へ配布され、各機器は、最新のCRLを入手する。なお、CRLについては、「American National Standard S Institute. American National Standard for financial services. ANS X9.57: Public Key Cryptography For the Financial Industry: Certificate Management. 1997.」に詳しく開示されている。

#### 【0027】

コンテンツ格納部109は、コンテンツ鍵を用いて暗号化された暗号化コンテンツを格納する。なお、コンテンツの取得方法は、本発明の主題ではないので、説明を省略するが、例として、インターネット、放送などを利用して取得する方法や、DVD等の記録媒体から取得する方法が有る。

10

コンテンツ鍵格納部118は、暗号化部110から暗号化コンテンツ鍵αを受け取り、格納する。

#### (3) 公開鍵暗号処理部105

公開鍵暗号処理部105は、他の機器と通信する際に、認証を行い、SAC(Secure Authentication Channel)を確立する。SACとは、暗号通信が可能となる安全な通信路を意味する。SACを確立する処理によって、認証相手の機器がCAに認められた正しい機器であることを確認できる。詳しい確立方法については後述する。また、公開鍵暗号処理部105は、認証によって、セッション鍵SKを共有する。

20

#### (4) 登録情報記憶部106

登録情報記憶部106は、耐タンパ領域であり、図3(a)に示す登録情報を記憶している。登録情報は、AD内サーバ100に登録可能な機器の台数及び登録されている機器のIDを管理する情報であり、機器ID、最大、登録台数、残数及びICカードIDから構成される。

#### 【0028】

機器IDは、AD内サーバ100に登録された機器のIDを記憶する領域である。AD内サーバ100に再生装置200及び車載機器300が登録されると、図3(b)のように、それぞれのIDであるID-2及びID-3が格納される。

30

最大は、AD内サーバ100に登録可能な機器の最大数を示し、本実施の形態では、2台である。登録台数は、既にAD内サーバ100に登録されている機器の台数を示す。残数は、AD内サーバ100に登録可能な台数を示す。

#### 【0029】

AD内サーバ100にクライアント機器が登録されていない初期の状態では、登録台数は「0」であり、残数は最大と同数である。AD内サーバ100に何れかのクライアント機器が登録されると、登録台数に「1」が加算され、残数から「1」が減算される。

ICカードIDは、AD内サーバ100に付属のICカード400のIDを予め記憶しており、書き換え出来ない。

#### (5) CSI生成部107、CSI格納部108

40

CSI格納部108は、外部からCSIを読むことが出来ない耐タンパ領域であり、AD内サーバ100に機器が登録されていない場合、未登録であることを示す値として「0」を記憶している。

#### 【0030】

CSI生成部107は、制御部101の制御の基、AD内サーバ100に最初に機器を登録する際に、CSIを生成する。また、登録した機器が全て脱退すると、CSI格納部108は、格納している値を「0」に書き換える。

ここでCSIは、CSI生成部107によって生成される任意のデータであり、本実施の形態では200ビットとする。なお、CSIのビット長は、これに限定されず、容易に推測されない、簡単に試すことが不可能な程度の長さであれば良い。

50

## 【0031】

C S I 生成部 107 は生成した C S I を C S I 格納部 108 に格納する。また、生成した C S I を、接続されている I C カード 400 に出力する。

なお、C S I は、定期的又は不定期に更新するとしても良い。

## (6) 暗号化部 110、119

暗号化部 119 は、再生装置 200 の登録の際、制御部 101 の制御の基、公開鍵暗号処理部 105 から受け取るセッション鍵 S K を用いて、C S I に暗号化アルゴリズム E を施して暗号化 C S I を生成し、生成した暗号化 C S I を入出力部 115 を介して再生装置 200 へ送信する。ここで、暗号化アルゴリズム S は、一例として D E S である。D E S については公知であるので、説明を省略する。

10

## 【0032】

暗号化部 110 は、コンテンツ鍵をコンテンツ鍵格納部 118 に格納する際、I D 格納部 111 から I D — 1 を読み出し、C S I 格納部 104 から C S I を読み出す。読み出した I D — 1 及び C S I をこの順で連結して暗号鍵 α とし、暗号鍵 α を用いてコンテンツ鍵に暗号化アルゴリズム E を施して暗号化して暗号化コンテンツ鍵 α を生成し、生成した暗号化コンテンツ鍵 α をコンテンツ鍵格納部 118 へ格納する。

## 【0033】

暗号化部 110 は、D V D 500 に暗号化コンテンツを書き込む際、制御部 101 の制御の基、登録情報記憶部 106 から登録情報の機器 I D から登録されている機器の I D である I D — 2 及び I D — 3 を読み出す。I D — 2 と C S I とをこの順で連結し、暗号鍵 b とし、I D — 3 と C S I とをこの順で連結して、暗号鍵 c とする。暗号鍵 b 及び暗号鍵 c をそれぞれ用いて暗号化コンテンツ鍵 b 及び暗号化コンテンツ鍵 c を生成し、D V D 500 に書き込む。

20

## (7) 復号部 117

復号部 117 は、制御部 101 の制御の基、I D 格納部 111 に記憶している I D — 1 を読み出し、C S I 格納部 108 に格納している C S I を読み出す。I D — 1 及び C S I をこの順で連結して復号鍵として用い、コンテンツ鍵格納部 118 から読み出した暗号化コンテンツ鍵 α に復号アルゴリズム D を施し、コンテンツ鍵を生成する。生成したコンテンツ鍵は、暗号化部 110 へ出力する。ここで、復号アルゴリズム D とは、暗号化アルゴリズム E の逆の処理をするアルゴリズムである。

30

## (8) 制御部 101、入力部 113、表示部 114

入力部 113 は、ユーザからの入力を受け付け、受け付けた入力を制御部 101 へ出力する。

## 【0034】

制御部 101 は、処理を開始する際、接続されている I C カード 400 から I C カードの I D を受信すると、受信した I D が登録情報の I C カード I D と一致するかどうかを確認する。一致しない場合は、接続された I C カードが付属の I C カードでないことを表示部 114 に表示し、処理を終了する。一致する場合のみ、以降の処理を継続する。

## &lt;再生装置 200 の登録&gt;

再生装置 200 から入出力部 115 を介して登録要求を受け取ると、制御部 101 は、公開鍵暗号処理部 105 を制御し、C S I の初期値「0」を用いて後述の方法で S A C を確立する。ここで、登録の際の認証に使用する「0」は、再生装置 200 が、何れの A D にも登録されていないことを示す。S A C を確立する際の機器認証の結果から、相手機器が未登録であるかどうかを判断する。認証相手の機器が保持する C S I の値が「0」である場合、認証に成功し、未登録であると判断する。認証相手の機器が保持する C S I の値が、「0」でない場合、制御部 101 は、相手の機器が既に何れかの A D に登録されていると判断する。

40

## 【0035】

未登録であると判断した場合、登録情報記憶部 106 から登録情報を読み出し、残数が「0」であるかどうかを判断する。残数が「0」でない場合、登録台数が「0」かどうかを判

50



断する。登録台数が「0」の場合、C S I 生成部 1 0 7 を制御して C S I を生成し、C S I 格納部 1 0 8 へ格納する。登録台数が「0」でなかった場合は、C S I 格納部 1 0 8 から C S I を読み出し、生成又は読み出した C S I を暗号化部 1 1 0 で暗号化して生成した暗号化 C S I を入出力部 1 1 5 を介して、再生装置 2 0 0 へ出力する。再生装置 2 0 0 から、C S I を受け取った事をする受領通知を受信すると、登録情報の登録台数に「1」を加算し、残数から「1」を減算し、処理を終了する。

#### 【0036】

機器認証の結果が失敗の場合、相手機器が登録済みである場合及び残数が「0」である場合は、登録できないことを示す登録不可通知を再生装置 2 0 0 へ送信し、処理を終了する。

10

また、C S I 生成部 1 0 7 で C S I を生成する際、I C カード 4 0 0 との間で S A C を確立してセッション鍵 S K を共有し、セッション鍵 S K を用いて生成した C S I に暗号化アルゴリズム E を施して暗号化 C S I を生成し、生成した暗号化 C S I を I C カード 4 0 0 へ送信する。

#### 【0037】

なお、上記登録処理の認証において、認証相手のクライアント機器の C S I が、C S I 格納部 1 0 8 に格納している C S I と一致するか否かを確認することによって、A D 内サーバ 1 0 0 が管理する A D に登録済みか否かを判断しても良い。クライアント機器の保持する C S I が、C S I 格納部 1 0 8 に格納している C S I と一致する場合、クライアント機器に対して、既に A D 内サーバ 1 0 0 に登録している旨を通知した後、登録の処理を終了するとしても良い。

20

#### 【0038】

また、クライアント機器が保持する C S I が、「0」でなく、C S I 格納部 1 0 8 に格納している C S I と異なる場合、他の A D に登録されていると判断する。クライアント機器が他の A D に登録されていると判断する場合、上記登録不可通知を送信後、登録の処理を終了するとしても良い。また、他の A D に登録済みであることを通知し、更に A D 内サーバ 1 0 0 への登録を続行するかを尋ね、続行する場合は、上記登録の処理を続行して、C S I 格納部 1 0 8 に格納している C S I を送信するとしても良い。この場合、クライアント機器は、A D 内サーバ 1 0 0 から C S I を受信すると、他の A D の C S I に、受信した C S I を上書きする。

30

#### 【0039】

また、上記登録処理の認証において、クライアント機器を不正な機器でないと判断した場合、クライアント機器が保持する C S I が如何なる値であっても登録処理を行い、C S I を送信するとしても良い。

#### <車載機器 3 0 0 の登録>

(a) 既に I D を確認済みの I C カード 4 0 0 が接続された状態で、入力部 1 1 3 から、C S I をコピーする旨の入力を受け付けると、制御部 1 0 1 は、残数が「0」か否かを判断し、「0」でなければ、I C カード 4 0 0 に、C S I のコピーを 1 回許可することを示す許可権利を送信する。制御部 1 0 1 は、I C カード 4 0 0 から受領通知を受け取ると、処理を終了する。

40

#### 【0040】

残数が「0」の場合は、表示部 1 1 4 にコピーできない旨を表示し、処理を終了する。

(b) I C カード 4 0 0 が接続され、I D を確認し、C S I をコピーしたことを示すコピー通知を受け取ると、コピー通知に含まれる、C S I のコピー先の I D を抽出し、登録情報に機器 I D として記憶する。また、I C カード 4 0 0 へ、コピー先の I D を受け取ったことを示す受領通知を送信する。

#### 【0041】

なお、ここでは、既に C S I が生成されているものとして説明したが、C S I が生成されていない場合は、前述の再生装置 2 0 0 を登録する際と同様に生成して I C カード 4 0 0 へ送信する。

50

## &lt;コンテンツ配布&gt;

入出力部 115 を介して再生装置 200 からコンテンツの配送要求を受信すると、制御部 101 は公開鍵暗号処理部 105 を制御して後述の方法で S A C を確立し、セッション鍵 S K を共有する。この S A C 確立の際の認証では、C S I 格納部 108 が格納している C S I を用いるため、認証に成功した場合、相手機器は A D 内サーバ 100 が生成した C S I を保持しているため、登録済みであると判断し、認証に失敗した場合、A D 内サーバ 100 に登録されていないと判断する。

## 【0042】

認証に失敗した場合、コンテンツを配送できないことを示す配送不可通知を再生装置 200 へ送信する。

認証に成功した場合、復号部 117 を制御して、コンテンツ鍵格納部 118 に格納している暗号化コンテンツ鍵 a を復号する。次に暗号化部 119 を制御して、セッション鍵 S K を用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵 S を生成させ、再生装置 200 へ送信する。また、コンテンツ格納部 109 から暗号化コンテンツを読み出し、再生装置 200 へ送信する。

## &lt;コンテンツをDVDに記録&gt;

入力部 113 からコンテンツを DVD 500 に記録する旨の入力を受け付けると、復号部 117 を制御してコンテンツ鍵格納部 118 に格納している暗号化コンテンツ鍵 a を復号させてコンテンツ鍵を生成させる。次に、暗号化部 119 を制御して登録情報に登録している I D — 2 及び I D — 3 をそれぞれ用いて生成した暗号鍵 b 及び暗号鍵 c を用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵 b 及び暗号化コンテンツ鍵 c を生成し、生成した暗号化コンテンツ鍵 b 及び c を DVD 500 へ書き込む。また、コンテンツ格納部 109 から暗号化コンテンツを読み出し、DVD 500 へ書き込む。

## 【0043】

なお、DVD 500 に固有の I D を基にして生成した暗号化鍵又は DVD 500 に固有の I D 及び C S I を基にして生成した暗号化鍵を用いて、コンテンツ鍵を暗号化するとしても良い。

## &lt;脱退&gt;

再生装置 200 から I D — 2 を含む脱退要求を受け取ると、公開鍵暗号処理部 105 を制御して後述の方法で S A C を確立する。この際、C S I 格納部 108 に格納している C S I を用いて認証を行う。S A C 確立の際の認証結果から、要求元の機器が登録済みであるか否かを判断し、未登録の場合脱退できないので、再生装置 200 へ未登録であることを示す未登録通知を送信する。

## 【0044】

登録済みの場合、再生装置 200 へ C S I を削除することを示す削除通知を送信する。再生装置 200 から C S I の削除が完了したことを示す完了通知を受信すると、登録情報の機器 I D から I D — 2 を削除し、登録台数から「1」減算し、残数に「1」を加算する。

## 1. 2. 再生装置 200 の構成

再生装置 200 は、図 4 に示すように、制御部 201、秘密鍵格納部 202、公開鍵証明書格納部 203、C R L 格納部 204、公開鍵暗号処理部 205、C S I 格納部 208、コンテンツ格納部 209、I D 格納部 211、入力部 213、入出力部 215、復号部 217、暗号化部 218、コンテンツ鍵格納部 219、復号部 220 及び再生部 221 から構成される。再生部 221 には、モニタ 251 及びスピーカ 252 が接続されている。

## 【0045】

再生装置 200 は、A D 内サーバ 100 と同様のコンピュータシステムであり、R A M 又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、再生装置 200 は、その機能を達成する。

## (1) 入出力部 215

10

20

30

40

50

入出力部 215 は、A D 内サーバ 100 とデータの送受信を行う。

(2) 秘密鍵格納部 202、公開鍵証明書格納部 203、C R L 格納部 204、C S I 格納部 208、I D 格納部 211

C R L 格納部 204 は、最新の C R L を格納している。

【0046】

I D 格納部 211 は、再生装置 200 に固有の I D である I D \_ 2 を記憶している。

C S I 格納部 208 は、耐タンパ領域であり、未登録であることを示す「0」を格納している。A D 内サーバ 100 に登録されると、A D 内サーバ 100 より取得した C S I を格納する。

公開鍵証明書格納部 203 は、C A より発行された公開鍵証明書 C e r t \_ 2 を格納する。この公開鍵証明書 C e r t \_ 2 は、再生装置 200 の公開鍵 P K \_ 2 及び再生装置 200 の I D \_ 2 と、それらに対する C A の署名データ S i g \_ C A 2 とを含む。

10

【0047】

秘密鍵格納部 202 は、耐タンパ領域であり、再生装置 200 の公開鍵 P K \_ 2 と対応する秘密鍵 S K \_ 2 を格納する。

(3) 公開鍵暗号処理部 205

公開鍵暗号処理部 205 は、A D 内サーバ 100 と通信する際に、後述の方法で S A C を確立し、セッション鍵 S K を共有する。共有したセッション鍵 S K を、復号部 217 へ出力する。

(4) 復号部 217、復号部 220

20

復号部 217 は、A D 内サーバ 100 からコンテンツを配送される際、公開鍵暗号処理部 205 で共有したセッション鍵 S K を用いて、A D 内サーバ 100 より配信された暗号化コンテンツ鍵 S に、復号アルゴリズム D を施してコンテンツ鍵を生成する。ここで、復号アルゴリズム D とは、暗号化アルゴリズム E と逆の処理を行う。

【0048】

また、一旦格納したコンテンツを再生する際、I D 格納部 211 から I D \_ 2 を読み出し、C S I 格納部 208 から C S I を読み出し、I D \_ 2 及び C S I をこの順で連結して復号鍵 b を生成する。生成した復号鍵 b を用いて、コンテンツ鍵格納部 219 から読み出した暗号化コンテンツ鍵 b に、復号アルゴリズム D を施してコンテンツ鍵を生成し、生成したコンテンツ鍵を復号部 220 へ出力する。

30

【0049】

復号部 220 は、コンテンツ格納部 209 に格納されている暗号化コンテンツを読み出し、復号部 217 から受け取るコンテンツ鍵を用いて、読み出した暗号化コンテンツに復号アルゴリズム D を施してコンテンツを生成し、生成したコンテンツを再生部 221 へ出力する。

(5) 暗号化部 218

暗号化部 218 は、A D 内サーバ 100 から取得したコンテンツを格納する際、I D 格納部 211 から I D \_ 2 を読み出し、C S I 格納部 208 から C S I を読み出す。I D \_ 2 及び C S I をこの順で連結して暗号鍵 b を生成し、生成した暗号鍵 b を用いて復号部 217 から受け取るコンテンツ鍵に暗号化アルゴリズム E を施して暗号化コンテンツ鍵 b を生成し、生成した暗号化コンテンツ鍵 b をコンテンツ鍵格納部 219 に出力する。

40

(6) コンテンツ格納部 209、コンテンツ鍵格納部 219

コンテンツ格納部 209 は、A D 内サーバ 100 から送信される暗号化コンテンツを格納する。

【0050】

コンテンツ鍵格納部 219 は、暗号化部 218 で暗号化された暗号化コンテンツ鍵 b を格納する。

(7) 制御部 201、入力部 213

<登録>

入力部 213 が登録処理を開始する旨の入力を受け付けると、制御部 201 は、I D 格

50

納部 211 から ID-2 を読み出し、ID-2 を含めた登録要求を、入出力部 215 を介して、AD 内サーバ 100 へ送信し、後述の方法で SAC を確立する。

#### 【0051】

制御部 201 は、AD 内サーバ 100 から、登録不可通知を受信すると、モニタ 251 に登録できない旨を表示し、登録の処理を終了する。

制御部 201 は、AD 内サーバ 100 から暗号化 CSI を受信すると、復号部 217 を制御して復号させて CSI を生成し、生成した CSI を CSI 格納部 208 に格納する。また、CSI を受領したことを示す受領通知を AD 内サーバ 100 へ送信する。

#### <コンテンツの配送>

入力部 213 がコンテンツを取得して再生する旨の入力を受け付けると、制御部 201 は、配送要求を AD 内サーバ 100 へ送信する。 10

#### 【0052】

制御部 201 は、AD 内サーバ 100 から配送不可通知を受信すると、モニタ 251 に配送できない旨を表示し、処理を終了する。

受信したコンテンツを再生する場合、制御部 201 は、AD 内サーバ 100 から暗号化コンテンツ鍵 S を受信すると、復号部 217 を制御して復号させてコンテンツ鍵を生成させる。また、AD 内サーバ 100 から暗号化コンテンツを受信すると、復号部 220 を制御し、暗号化コンテンツを復号してコンテンツを生成させ、再生部 221 にコンテンツを再生させる。

#### <コンテンツを蓄積してから再生>

入力部 213 がコンテンツを取得して蓄積する旨の入力を受け付けると、制御部 201 は、上記と同様に処理してコンテンツを取得する。コンテンツを取得すると、制御部 201 は、AD 内サーバ 100 から受信した暗号化コンテンツ鍵 S を復号部 217 に復号させ、復号したコンテンツ鍵を暗号化部 218 を制御して暗号化させ、暗号化コンテンツ鍵 b としてコンテンツ鍵格納部 219 に格納する。また、AD 内サーバ 100 から暗号化コンテンツを受信すると、コンテンツ格納部 209 に格納する。 20

#### 【0053】

入力部 213 がコンテンツ格納部 209 に格納したコンテンツを再生する旨の入力を受け付けると、制御部 201 は、復号部 217 を制御して暗号化コンテンツ鍵 b を復号させ、復号部 220 に暗号化コンテンツを復号させてコンテンツを生成し、再生部 221 にコンテンツを再生させる。 30

#### <脱退>

入力部 213 が脱退処理を開始する旨の入力を受け付けると、制御部 101 は、後述の方法で SAC を確立する。

#### 【0054】

制御部 201 は、AD 内サーバ 100 から未登録通知を受信すると、AD 内サーバ 100 に登録されていないことをモニタ 251 に表示して処理を終了する。

制御部 201 は、AD 内サーバ 100 から削除通知を受信すると、CSI 格納部 208 に格納している CSI を削除し、未登録を示す「0」を格納する。また、削除が完了したことを AD 内サーバ 100 に通知する削除完了通知を送信する。 40

#### (8) 再生部 221

再生部 221 は、復号部 220 から受け取るコンテンツから映像信号を生成し、生成した映像信号をモニタ 251 へ出力する。また、受け取ったコンテンツから音声信号を生成し、生成した音声信号をスピーカ 252 へ出力する。

#### 1.3 車載機器 300 の構成

車載機器 300 は図 5 に示すように、制御部 301、秘密鍵格納部 302、公開鍵証明書格納部 303、CRL 格納部 304、公開鍵暗号処理部 305、CSI 格納部 308、ID 格納部 311、ドライブ部 312、入力部 313、入出力部 316、復号部 317、318、320、再生部 321、モニタ 322 及びスピーカ 323 から構成される。

#### 【0055】

車載機器 300 は、A D 内サーバ 100 と同様のコンピュータシステムであり、R A M 又はハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、車載機器 300 は、その機能を達成する。

(1) ドライブ部 312、入出力部 316

ドライブ部 312 は、D V D 500 から暗号化コンテンツ鍵 c を読み出し、復号部 318 へ出力する。また、暗号化コンテンツを読み出し、復号部 320 へ出力する。

【0056】

入出力部 316 は、制御部 301 の制御の基、I C カード 400 とデータの送受信を行う。

10

(2) 秘密鍵格納部 302、公開鍵証明書格納部 303、C R L 格納部 304、C S I 格納部 308、I D 格納部 311

C R L 格納部 304 は、最新の C R L を格納する。

【0057】

I D 格納部 311 は、車載機器 300 に固有の I D である I D \_ 3 を記憶している。

C S I 格納部 308 は、耐タンパ領域であり、未登録を示す「0」を格納している。I C カード 400 から、A D 内サーバ 100 により生成された C S I を受け取ると、受け取った C S I を格納する。

公開鍵証明書格納部 303 は、C A より発行された公開鍵証明書 C e r t \_ 3 を格納する。この公開鍵証明書 C e r t \_ 3 は、車載機器 300 の公開鍵 P K \_ 3 及び I D \_ 3 と、それらに対する C A の署名データ S i g \_ C A 3 とを含む。

20

【0058】

秘密鍵格納部 302 は、耐タンパ領域であり、公開鍵 P K \_ 3 と対応する秘密鍵 S K \_ 3 を格納している。

(3) 公開鍵暗号処理部 305

公開鍵暗号処理部 305 は、制御部 301 の制御の基、I C カード 400 と認証を行い、後述の方法で S A C を確立する。また、この際に共有したセッション鍵 S K を復号部 317 へ出力する。

(4) 復号部 317、318、320

復号部 317 は、制御部 301 の制御の基、I C カード 400 から暗号化 C S I を受け取ると、公開鍵暗号処理部 305 から受け取るセッション鍵 S K を用いて、暗号化 C S I に復号アルゴリズム D を施して C S I を生成し、生成した C S I を C S I 格納部 308 へ出力する。

30

【0059】

復号部 318 は、コンテンツを再生する際、ドライブ部から暗号化コンテンツ鍵 c を受け取ると、I D 格納部 311 から I D \_ 3 を読み出し、C S I 格納部 308 から C S I を読み出す。読み出した I D \_ 3 及び C S I をこの順で連結して復号鍵 c を生成する。復号鍵 c を用いて暗号化コンテンツ鍵 c に復号アルゴリズム D を施してコンテンツ鍵を生成し、生成したコンテンツ鍵を復号部 320 へ出力する。

【0060】

復号部 320 は、ドライブ部 312 から暗号化コンテンツを受け取り、復号部 318 からコンテンツ鍵を受け取る。受け取ったコンテンツ鍵を用いて暗号化コンテンツに復号アルゴリズム D を施してコンテンツを生成し、生成したコンテンツを再生部 321 へ出力する。

40

(5) 制御部 301、入力部 313

制御部 301 は、I C カード 400 が接続されると、S A C を確立する。この際、C S I 格納部 308 に格納されている「0」を C S I として用いる。機器認証に失敗した場合、処理を終了する。また、I C カード 400 から登録済通知を受け取った場合、登録済みであることをモニタ 322 に表示して処理を終了する。制御部 301 は、入出力部 316 を介して I C カード 400 から暗号化 C S I を受け取ると、復号部 317 を制御して復号

50

させてC S Iを生成し、生成したC S IをC S I格納部308に格納する。また、C S Iを受領したことを示す受領通知をI Cカード400へ送信する。

#### 【0061】

なお、車載機器300から他の機器へのC S Iのコピーは行わない。

制御部301は、入力部313からD V D 5 0 0に記録されているコンテンツを視聴する旨の入力を受け付けると、ドライブ部312を制御してD V D 5 0 0から暗号化コンテンツ鍵c及び暗号化コンテンツを読み出す。復号部318で暗号化コンテンツ鍵cを復号させてコンテンツ鍵を生成させ、復号部320で暗号化コンテンツを復号させてコンテンツを生成させる。また、再生部321を制御してコンテンツを再生させる。

#### (6) 再生部321、モニタ322、スピーカ323

再生部321は、受け取ったコンテンツから映像信号を生成してモニタ322へ出力し、音声信号を生成してスピーカ323へ出力し、コンテンツを再生する。

#### 1. 4 I Cカード400の構成

I Cカード400は図6に示すように、制御部401、秘密鍵格納部402、公開鍵証明書格納部403、C R L格納部404、公開鍵暗号処理部405、C S I格納部408、I D格納部411、入出力部416、復号部417、暗号化部418及びI D記憶部420から構成される。

#### 【0062】

I Cカード400は、A D内サーバ100及び車載機器300に接続可能である。車載機器300のような、A D内サーバ100と接続できない機器をA D内の機器として登録する際に用いる。

(1) 秘密鍵格納部402、公開鍵証明書格納部403、C R L格納部404、C S I格納部408、I D格納部411、I D記憶部420

C R L格納部404は、最新のC R Lを格納する。

#### 【0063】

I D格納部411は、I Cカード400に固有のI DであるI D—4を記憶している。

C S I格納部408は、耐タンパ領域であり、A D内サーバ100にクライアント機器が登録されていない場合、未登録を示す「0」を格納している。A D内サーバ100によりC S Iが生成されると、A D内サーバ100より取得したC S Iと、コピー回数である「0」とを対応付けて記憶する。ここで、コピー回数とは、他のクライアント機器へC S Iを通知することを許可された回数である。

#### 【0064】

公開鍵証明書格納部403は、C Aより発行された公開鍵証明書C e r t—4を格納する。この公開鍵証明書C e r t—4は、I Cカード400の公開鍵P K—4及びI D—4と、それらに対するC Aの署名データS i g—C A4とを含む。

秘密鍵格納部402は、耐タンパ領域であり、公開鍵P K—4と対応する秘密鍵S K—4を格納している。

#### 【0065】

I D記憶部420は、C S Iのコピー先のI Dを記憶する領域である。

#### (2) 公開鍵暗号処理部405

公開鍵暗号処理部405は、制御部401の制御の基、A D内サーバ100とS A Cを確立し、セッション鍵S Kを共有し、共有したセッション鍵S Kを復号部417へ出力する。

#### 【0066】

また、車載機器300との間にS A Cを確立してセッション鍵S Kを共有し、共有したセッション鍵S Kを暗号化部418へ出力する。

#### (3) 復号部417

復号部417は、入出力部416を介して暗号化C S Iを受け取ると、制御部401の制御の基、公開鍵暗号処理部405から受け取るセッション鍵S Kを用いて暗号化C S Iに復号アルゴリズムDを施してC S Iを生成する。生成したC S IをC S I格納部408

10

20

30

40

50

へ格納する。

(4) 暗号化部 418

暗号化部 418 は、制御部 401 の制御の基、C S I 格納部 408 から C S I を読み出し、公開鍵暗号処理部 405 からセッション鍵 S K を受け取り、セッション鍵 S K を用いて C S I に暗号化アルゴリズム E を施して暗号化 C S I を生成し、生成した暗号化 C S I を車載機器 300 へ送信する。

(5) 制御部 401、入出力部 416

A D 内サーバ 100 に接続されると、制御部 401 は、I D 格納部 411 から I D \_ 4 を読み出し、読み出した I D \_ 4 を A D 内サーバ 100 へ送信する。

【0067】

10

A D 内サーバ 100 から C S I を受け取る際、制御部 401 は、公開鍵暗号処理部 405 を制御して A D 内サーバ 100 との間に S A C を確立してセッション鍵 S K を共有し、暗号化 C S I を受信すると、復号部 417 で復号させて C S I を生成し、C S I 格納部 408 に C S I を格納する。

車載機器 300 を登録する際、制御部 401 は、A D 内サーバ 100 から許可権利を受信すると、C S I と対応付けて格納しているコピー回数に「1」を加算し、A D 内サーバ 100 に、受領通知を送信する。

【0068】

車載機器 300 に接続されると、公開鍵暗号処理部 405 を制御して S A C を確立し、セッション鍵 S K を共有する。この際、C S I として初期値「0」を用いて認証を行い、認証結果から、車載機器 300 が未登録であるか否かを判断する。認証が失敗の場合、登録済みであると判断し、登録済通知を送信し、処理を終了する。認証が成功の場合、未登録であると判断し、認証の際に受け取る、車載機器 300 の I D \_ 3 を I D 記憶部 420 に記憶する。制御部 401 は、C S I 格納部 408 に格納している C S I を読み出し、暗号化部 418 で暗号化して暗号化 C S I を生成し、車載機器 300 へ送信する。制御部 401 は、車載機器 300 から受領通知を受け取ると、コピー回数から「1」減算し、処理を終了する。

20

【0069】

制御部 401 は、A D 内サーバ 100 に接続されると、I D 格納部 411 から I D \_ 4 を読み出して A D 内サーバ 100 へ送信する。また、I D 記憶部 420 から C S I のコピー先の I D を読み出し、読み出した I D を含むコピー通知を A D 内サーバ 100 へ送信する。A D 内サーバ 100 から受領通知を受け取ると、処理を終了する。

30

2. グループ形成管理システム 1 の動作

2. 1 S A C の動作

S A C を確立する際の動作について、図 7、8 を用いて説明する。

【0070】

なお、この S A C の確立方法は、A D 内サーバ 100、再生装置 200、車載機器 300 及び I C カード 400 の何れの機器同士の認証にも利用するため、ここでは認証を行う機器を、機器 A 及び機器 B と称する。また、認証で使用する C S I は、未登録を示す「0」の場合と、A D 内サーバ 100 が生成した値の場合とが有るが、ここでは全て C S I と

40

【0071】

ここで、 $Gen()$  を鍵生成関数とし、 $Y$  を、システム固有のパラメータとする。また、鍵生成関数  $Gen()$  は、 $Gen(x, Gen(y, z)) = Gen(y, Gen(x, z))$  の関係を満たすものとする。なお、鍵生成関数は、任意の公知技術で実現可能なため、その詳細についてここでは言及しない。その一例として、文献(1)池野信一、小山謙二、「現代暗号理論」、電気通信学会にディフィーヘルマン(DH)型公開鍵配送法が開示されている。

【0072】

機器 A は、公開鍵証明書  $Ce r t _ A$  を読み出し(ステップ S 11)、機器 B へ送信す

50

る（ステップS12）。

公開鍵証明書Cert-Aを受け取った機器Bは、CAの公開鍵PK-CAを用いて、公開鍵証明書Cert-Aに含まれる署名データSig-CAに対して、署名検証アルゴリズムVを施して署名検証する（ステップS13）。検証結果が失敗の場合（ステップS14でNO）、処理を終了する。検証結果が成功の場合（ステップS14でYES）、CRLを読み出し（ステップS15）、公開鍵証明書Cert-Aに含まれて受け取ったID-AがCRLに登録されているか否かを判断する（ステップS16）。登録されていると判断する場合（ステップS16でYES）、処理を終了する。登録されていないと判断する場合（ステップS16でNO）、機器Bの公開鍵証明書Cert-Bを読み出し（ステップS17）、機器Aへ送信する（ステップS18）。

10

【0073】

機器Aは、公開鍵証明書Cert-Bを受け取ると、公開鍵PK-CAを用いて公開鍵証明書Cert-Bに含まれる署名データSig-CAに対して、署名検証アルゴリズムVを施して署名検証する（ステップS19）。検証結果が失敗の場合（ステップS20でNO）、処理を終了する。検証結果が成功の場合（ステップS20でYES）、CRLを読み出し（ステップS21）、公開鍵証明書Cert-Bに含まれて受け取ったID-BがCRLに登録されているか否かを判断する（ステップS22）。登録されていると判断する場合（ステップS22でYES）、処理を終了する。登録されていないと判断する場合（ステップS22でNO）、処理を継続する。

【0074】

20

機器Bは、乱数Cha-Bを生成し（ステップS23）、機器Aへ送信する（ステップS24）。

機器Aは、乱数Cha-Bを受け取ると、Cha-BとCSIとをこの順で連結してCha-B||CSIを生成し（ステップS25）、生成したCha-B||CSIに、機器Aの秘密鍵SK-Aを用いて署名生成アルゴリズムSを施して署名データSig-Aを生成し（ステップS26）、生成した署名データSig-Aを機器Bへ送信する（ステップS27）。

【0075】

機器Bは、署名データSig-Aを受け取ると、ステップS12でCert-Aに含んで受け取ったPK-Aを用いて受け取った署名データSig-Aに署名検証アルゴリズムVを施して署名検証し（ステップS28）、検証結果が失敗の場合は（ステップS29でNO）、処理を終了し、成功の場合（ステップS29でYES）は処理を継続する。

30

機器Aは、乱数Cha-Aを生成し（ステップS30）、機器Bへ送信する（ステップS31）。

【0076】

機器Bは、受け取ったCha-AとCSIとをこの順で連結してCha-A||CSIを生成し（ステップS32）、生成したCha-A||CSIに、機器Bの秘密鍵SK-Bを用いて署名生成アルゴリズムSを施して署名データSig-Bを生成し（ステップS33）、生成した署名データSig-Bを機器Aへ送信する（ステップS34）。

機器Aは、署名データSig-Bを受け取ると、ステップS18でCert-Bに含んで受け取ったPK-Bを用いて署名データSig-Bに署名検証アルゴリズムVを施して署名検証し（ステップS35）、検証結果が失敗の場合（ステップS36でNO）、処理を終了する。成功の場合（ステップS36でYES）、乱数「a」を生成し（ステップS37）、生成した「a」を用いて $Key-A = Gen(a, Y)$ を生成し（ステップS38）、生成したKey-Aを機器Bへ送信する（ステップS39）。

40

【0077】

機器Bは、Key-Aを受け取ると、乱数「b」を生成し（ステップS40）、生成した乱数「b」を用いて $Key-B = Gen(b, Y)$ を生成する（ステップS41）。生成したKey-Bを機器Aへ送信する（ステップS42）。また、生成した乱数「b」と、受け取ったKey-Aとを用いて、 $Key-AB = Gen(b, Key-A) = Gen$

50



( $b$ ,  $Gen(a, Y)$ ) を生成し (ステップ S43)、 $Key\_AB$  と、 $CSI$  を用いてセッション鍵  $SK = Gen(CSI, Key\_AB)$  を生成する (ステップ S44)。

#### 【0078】

機器 A は、 $Key\_B$  を受け取ると、生成した乱数「 $a$ 」と受け取った  $Key\_B$  とから  $Key\_AB = Gen(a, Key\_B) = Gen(a, Gen(b, Y))$  を生成し (ステップ S45)、生成した  $Key\_AB$  と  $CSI$  を用いて、セッション鍵  $SK = Gen(CSI, Key\_AB)$  を生成する (ステップ S46)。

#### 2. 2 再生装置 200 登録の動作

AD 内サーバ 100 に、再生装置 200 を登録する際の動作を図 9 を用いて説明する。 10

#### 【0079】

なお、AD 内サーバ 100 は、IC カード 400 が接続され、IC カード 400 が付属の IC カードであるかを既に確認している。

再生装置 200 は、入力部 213 から登録処理を開始する旨の入力を受け付けると (ステップ S51)、ID 格納部 211 から ID\_2 を読み出し (ステップ S52)、ID\_2 を含めて登録要求を AD 内サーバ 100 へ送信する (ステップ S53)。

#### 【0080】

AD 内サーバ 100 を機器 A とし、再生装置 200 を機器 B として、前述の方法で SAC を確立する (ステップ S54)。この際、AD 内サーバ 100 は、 $CSI$  として「0」を使用し、再生装置 200 は、 $CSI$  格納部 208 に格納している  $CSI$  を使用する。 20

AD 内サーバ 100 は、ステップ S35 の署名検証で、 $CSI$  として「0」を用いて署名検証するので、検証結果が成功の場合は未登録であると判断し、失敗の場合は、登録済みであると判断する。再生装置 200 が未登録であると判断する場合、登録情報を読み出し (ステップ S55)、残数が「0」か否かを判断する (ステップ S56)。「0」である場合 (ステップ S56 で YES)、登録不可通知を再生装置 200 へ送信する (ステップ S57)。残数が「0」でない場合 (ステップ S56 で NO)、登録台数が「0」であるか否かを判断する (ステップ S58)。「0」である場合 (ステップ S58 で YES)、 $CSI$  生成部 107 で  $CSI$  を生成する (ステップ S59)。登録台数が「0」でない場合 (ステップ S58 で NO)、 $CSI$  格納部 108 から  $CSI$  を読み出す (ステップ S60)。生成又は読み出した  $CSI$  に、暗号化部 119 でセッション鍵  $SK$  を用いて暗号化アルゴリズム E を施して暗号化して暗号化  $CSI$  を生成し (ステップ S61)、暗号化  $CSI$  を再生装置 200 へ送信する (ステップ S62)。 30

#### 【0081】

再生装置 200 は、登録不可通知を受信した場合、登録できないことをモニタ 251 に表示し (ステップ S63)、処理を終了する。暗号化  $CSI$  を受信した場合、復号部 217 で暗号化  $CSI$  を復号して  $CSI$  を生成し (ステップ S64)、 $CSI$  格納部 208 に格納する (ステップ S65)。また、AD 内サーバ 100 に受領通知を送信する (ステップ S66)。

#### 【0082】

再生装置 200 から受領通知を受信すると、登録情報の機器 ID に、ID\_2 を書き込み、登録台数に「1」を加算し、残数から「1」を減算する (ステップ S67)。 40

#### 2. 3 車載機器 300 登録の動作

(1) AD 内サーバ 100 から IC カード 400 に  $CSI$  のコピーを許可する際の動作について、図 10 を用いて説明する。

#### 【0083】

IC カード 400 が AD 内サーバ 100 に接続されると、IC カード 400 は、ID 格納部 411 から ID\_4 を読み出し (ステップ S71)、AD 内サーバ 100 に ID\_4 を送信する (ステップ S72)。

AD 内サーバ 100 は、ID\_4 を受信すると、登録情報から IC カード ID を読み出し (ステップ S73)、受信した ID と読み出した ID とが一致するか否かを判断する ( 50

ステップS74)。一致しない場合(ステップS74でNO)、接続されたICカードが付属のICカードでないことを表示部114に表示し(ステップS75)、処理を終了する。一致する場合(ステップS74でYES)、処理を継続する。このように、接続されたICカードが付属のICカードであるか確認し、確認が済むと入力を受け付けるまで待機する。

#### 【0084】

入力部113が、ICカード400にCSIを記録する旨の入力を受け付けると(ステップS76)、制御部101は、登録情報記憶部106から残数を読み出して(ステップS77)、残数が「0」か否かを判断し(ステップS78)、「0」である場合は(ステップS78でYES)、登録出来ないことを表示部114に表示する(ステップS79)。残数が「0」でない場合(ステップS78でNO)、ICカード400にCSIのコピーを1回許可する許可権利を送信する(ステップS80)。

10

#### 【0085】

ICカード400は、AD内サーバ100から許可権利を受信すると、コピー回数に「1」を加算し(ステップS81)、AD内サーバ100に受領通知を送信する(ステップS82)。

AD内サーバ100は、受領通知を受信すると、登録情報の登録台数に「1」を加算し、残数から「1」を減算し(ステップS83)、処理を終了する。

(2) ICカード400から車載機器300にCSIをコピーする際の動作について、図11を用いて説明する。

20

#### 【0086】

ICカード400が車載機器300に接続されると、ステップS71～75の処理を行い、ICカードIDを確信する。また、ICカード400を機器Aとして、車載機器300を機器BとしてSACの確立処理を行い、セッション鍵SKを共有する(ステップS91)。この際、ICカード400はCSIの初期値である「0」を用いて認証を行い、車載機器300は、CSI格納部308に格納している値を用いて認証を行う。

#### 【0087】

ICカード400の制御部401は、ステップS35の署名検証で、CSIとして「0」を用いて署名検証するので、検証結果が成功の場合は未登録であると判断し、失敗の場合は、登録済みであると判断する。登録済みと判断する場合(ステップS92でNO)、車載機器300へ登録不可通知を送信し(ステップS93)、処理を終了する。未登録であると判断する場合(ステップS92でYES)、ステップS18で受け取る、車載機器300のID-3をID記憶部420に記憶する(ステップS94)。暗号化部418は、公開鍵暗号処理部405からセッション鍵SKを受け取ると、CSI格納部408からCSIを読み出す(ステップS95)。セッション鍵SKを用いてCSIを暗号化して暗号化CSIを生成し(ステップS96)、生成した暗号化CSIを入出力部416を介して車載機器300へ送信する(ステップS97)。

30

#### 【0088】

車載機器300の制御部301は、ICカード400から登録不可通知を受け取った場合、登録済みであることをモニタ322に表示し(ステップS98)、登録処理を終了する。ICカード400から暗号化CSIを受信した場合、復号部317は公開鍵暗号処理部305からセッション鍵SKを受け取り、セッション鍵SKを用いて暗号化CSIを復号してCSIを生成し(ステップS99)、生成したCSIをCSI格納部308へ格納する(ステップS100)。また、受領通知をICカード400へ送信する(ステップS101)。

40

#### 【0089】

ICカード400は、車載機器300から受領通知を受信すると、コピー回数から「1」を減算し(ステップS102)、処理を終了する。

(3) CSIをコピーしたことをAD内サーバ100に通知する際の動作

ICカード400がAD内サーバ100に接続されると、AD内サーバ100は、IC

50

カード４００のＩＤを確認して付属のＩＣカードであるか確認し、確認が済むと入力を受け付けるまで待機する。

【００９０】

ＩＣカード４００は、ＩＤ記憶部４２０からコピー先のＩＤであるＩＤ—３を読み出し、ＩＤ—３を含むコピー通知をＡＤ内サーバ１００へ送信する。

ＡＤ内サーバ１００は、コピー通知を受信すると、コピー通知に含まれるＩＤ—３を、登録情報に機器ＩＤとして記憶する。また、ＩＣカード４００へ、受領通知を送信し、処理を終了する。

【００９１】

ＩＣカード４００は、ＡＤ内サーバ１００から受領通知を受信すると、処理を終了する 10

## 2. 4 コンテンツ配送の動作 1

ＡＤ内サーバ１００から再生装置２００へコンテンツを配信し、再生する際の動作を、図１２を用いて説明する。

【００９２】

再生装置２００は、入力部２１３からコンテンツを取得する旨の入力を受け付けると（ステップＳ１２１）、ＡＤ内サーバ１００へコンテンツの配送要求を送信する（ステップＳ１２２）。

ＡＤ内サーバ１００及び再生装置２００は、ＳＡＣを確立する（ステップＳ１２３）。この際、それぞれＣＳＩ格納部に格納しているＣＳＩを用いて認証を行う。 20

【００９３】

ＡＤ内サーバ１００は、ステップＳ３５の処理で、再生装置２００が同一ＡＤ内の機器であることを確認する。

認証が失敗の場合（ステップＳ１２４でＮＯ）、ＡＤ内サーバ１００は、再生装置２００へ配送不可通知を送信し（ステップＳ１２５）、処理を終了する。認証が成功の場合（ステップＳ１２４でＹＥＳ）、ＡＤ内サーバ１００は、コンテンツ鍵格納部１１８から暗号化コンテンツ鍵αを読み出し（ステップＳ１２６）、復号部１１７で復号し（ステップＳ１２７）、更に、暗号化部１１０にて、認証の際に共有したセッション鍵ＳＫを用いて暗号化して暗号化コンテンツ鍵Ｓを生成し（ステップＳ１２８）、生成した暗号化コンテンツ鍵Ｓを再生装置２００へ送信する（ステップＳ１２９）。また、コンテンツ格納部１ 30  
０９から暗号化コンテンツを読み出し（ステップＳ１３０）、再生装置２００へ送信する（ステップＳ１３１）。

【００９４】

再生装置２００は、配送不可通知を受信した場合、モニタ２５１に配送できない旨を表示し（ステップＳ１３２）、処理を終了する。暗号化コンテンツ鍵Ｓを受信した場合、セッション鍵ＳＫを用いて復号部２１７にて復号してコンテンツ鍵を生成し（ステップＳ１ 33  
３３）、生成したコンテンツ鍵を復号部２２０へ出力する。復号部２２０は、復号部２１７から受け取ったコンテンツ鍵を用いて、ＡＤ内サーバ１００から受け取る暗号化コンテンツに復号アルゴリズムＤを施してコンテンツを生成し（ステップＳ１３４）、再生部２ 40  
２１へ出力する。再生部２２１は、受け取ったコンテンツから映像信号及び音声信号を生成してモニタ２５１及びスピーカ２５２へ出力し、コンテンツを再生する（ステップＳ１３５）。

## 2. 5 コンテンツ配送の動作 2

ＡＤ内サーバ１００から受信したコンテンツを、再生装置２００内に一旦蓄積してから再生する際の動作を、図１３を用いて説明する。

【００９５】

ステップＳ１２１からステップＳ１３０までは同様の処理を行う。

復号部２１７は、暗号化コンテンツ鍵Ｓを復号してコンテンツ鍵を生成し（ステップＳ 50  
１４１）、生成したコンテンツ鍵を暗号化部２１８へ出力する。暗号化部２１８は、ＣＳＩ格納部２０８からＣＳＩを読み出し、ＩＤ格納部２１１からＩＤ—２を読み出す（ステ

ステップS142)。ID-2及びCSIをこの順で連結してID-2||CSIを生成し(ステップS143)暗号化鍵bとする。生成した暗号化鍵bを用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵bを生成し(ステップS144)、暗号化コンテンツ鍵bをコンテンツ鍵格納部219へ格納する(ステップS145)。また、AD内サーバ100から暗号化コンテンツを受信すると、コンテンツ格納部209へ格納する(ステップS146)。

#### 【0096】

入力部213から格納したコンテンツを再生する旨の入力を受け付けると(ステップS147)、復号部217は、コンテンツ鍵格納部219から暗号化コンテンツ鍵bを読み出す(ステップS148)。また、CSI格納部208からCSIを読み出し、ID格納部211からID-2を読み出し(ステップS149)、ID-2及びCSIを連結してID-2||CSIを生成し(ステップS150)、復号鍵とする。生成した復号鍵を用いて暗号化コンテンツ鍵bに復号アルゴリズムDを施してコンテンツ鍵を生成し(ステップS151)、生成したコンテンツ鍵を復号部220へ出力する。復号部220及び再生部221は、ステップS132～ステップS133の処理を行い、コンテンツを再生する。

### 2.6 DVDに記録する際の動作

AD内サーバ100でDVD500にコンテンツを書き込む際の動作を、図14を用いて説明する。

#### 【0097】

AD内サーバ100は、入力部113からコンテンツをDVDに記録する旨の入力を受け付けると(ステップS161)、コンテンツ鍵格納部118から暗号化コンテンツ鍵aを読み出し(ステップS162)、ID格納部111からID-1を読み出し、CSI格納部108からCSIを読み出す(ステップS163)。復号部117は、ID-1とCSIとを連結して復号鍵を生成し(ステップS164)、生成した復号鍵を用いて暗号化コンテンツ鍵aを復号してコンテンツ鍵を生成し(ステップS165)、生成したコンテンツ鍵を暗号化部110へ出力する。暗号化部110は、コンテンツ鍵を受け取ると、登録情報記憶部106から機器IDを読み出し、CSI格納部108からCSIを読み出す(ステップS166)。読み出したID-2とCSIとを連結して暗号鍵bを生成し、ID-3とCSIとを連結して暗号鍵cを生成する(ステップS167)。生成した暗号鍵b及び暗号鍵cをそれぞれ用いてコンテンツ鍵を暗号化して暗号化コンテンツ鍵b及び暗号化コンテンツ鍵cを生成する(ステップS168)。生成した暗号化コンテンツ鍵b及び暗号化コンテンツ鍵cをDVD500に書き込む(ステップS169)。また、コンテンツ格納部109から暗号化コンテンツを読み出し(ステップS170)、DVD500に書き込む(ステップS171)。

### 2.7 再生装置200脱退の動作

AD内サーバ100から再生装置200が脱退する際の動作を図15を用いて説明する。

#### 【0098】

なお、AD内サーバ100は、ICカード400が接続され、既にICカードIDを確認している。

再生装置200は、入力部213から脱退する旨の入力を受け付けると(ステップS181)、ID格納部211からID-2を読み出し(ステップS182)、ID-2を含めて脱退要求をAD内サーバ100に送信する(ステップS183)。

#### 【0099】

AD内サーバ100及び再生装置200は、認証を行い、SACを確立する(ステップS184)。この際、それぞれCSI格納部に格納しているCSIを用いて認証を行う。

AD内サーバ100は、ステップS35の処理で、再生装置200がAD内の機器として登録しているか否かを判断し、未登録の場合(ステップS185でNO)、未登録通知を再生装置200へ送信する(ステップS186)。登録済みの場合は(ステップS18

10

20

30

40

50

5でYES)、CSI削除通知を送信する(ステップS187)。

#### 【0100】

再生装置200は、未登録通知を受信すると、モニタ322に未登録であることを表示し(ステップS188)、処理を終了する。削除通知を受信すると、CSI格納部208からCSIを削除する(ステップS189)。また、削除完了通知をAD内サーバ100へ送信する(ステップS190)。

AD内サーバ100は、削除完了通知を受信すると、機器IDからID-2を削除し、登録台数から「1」を減算し、残数に「1」を加算する(ステップS191)。

#### 3. 鍵配信方法の変形例

上記のグループ形成管理システム1において、グループ形成後、コンテンツ鍵の配信を行っている。上記に示した鍵配信方法では、コンテンツ鍵の配信時に制限を設けていなかったが、ここでは、コンテンツ鍵の配信時に制限を設けた鍵配信方法について、説明する

10

#### 【0101】

なお、ここでは、鍵の配信を行うシステムを、鍵配信システムという。

#### 3. 1 鍵配信システム1000の構成

ここでは、鍵配信システム1000の構成について説明する。

鍵配信システム1000は、図16に示すように、コンテンツサーバ1001、記録媒体1002、再生装置1003、再生装置1004、ゲートウェイ(以下、「GW」という。)1007とから構成され、1つのホームネットワークを形成している。このホームネットワークが、上記のグループとなる。ここで、ホームネットワークとは、同一のサブネットが割り当てられているネットワークシステムである。

20

#### 【0102】

GW1007は、ネットワーク上で、通信を可能にする機器である。

コンテンツサーバ1001と再生装置1003及び再生装置1004は、GW1007を介してホームネットワークを形成しており、さらに、インターネットにより再生装置1005とネットワーク接続されている。

コンテンツサーバ1001は、放送局1006よりコンテンツを受信、又は図示していないが、インターネット上のコンテンツ配信サイトよりコンテンツを取得する。なお、ここでは、便宜上、放送局1006よりコンテンツを取得することとして話を進める。コンテンツサーバ1001は、取得したコンテンツを暗号化するためにコンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、取得したコンテンツを暗号化し、暗号化コンテンツを生成し、生成した暗号化コンテンツを、暗号化コンテンツを識別する識別子である情報IDと対応付けて格納する。ここで、コンテンツを暗号化する方法は、共通鍵暗号である。これは、ある情報の暗号化及び復号において、同一の鍵を用いて行うことであり、一例として、AES(Advanced Encryption Standard)である。AESについては、公知であるので説明を省略する。

30

#### 【0103】

ここで、格納された暗号化コンテンツの複製には、制限を設けない。暗号化コンテンツの複製時には、暗号化コンテンツと情報IDとの組にて複製される。なお、本実施の形態では、再生装置1004及び記録媒体1002は、コンテンツサーバ1001にて生成された暗号化コンテンツを少なくとも1つ以上記憶しているものとする。

40

また、コンテンツサーバ1001は、コンテンツ鍵と、コンテンツ鍵を配信できる数とを対応付けて管理すること、暗号化コンテンツの利用を制限する。

#### 【0104】

コンテンツサーバ1001、再生装置1004及び記録媒体1002は、鍵配信システム1000内のみに有効な共通秘密情報を保持しており、コンテンツサーバ1001は、コンテンツ鍵の配信要求を受け付けた場合には、要求元である再生装置1004又は記録媒体1002と、この共通秘密情報を用いて認証を行い、コンテンツ鍵配信の正当性の確認、つまり、配信先の再生装置が正当な装置であるか、又は配信先の記録媒体が正当な記

50

録媒体であるかを判断する。

【0105】

ここで用いる認証方法は、一例として、ゼロ知識証明を利用したチャレンジアンドレスポンス型のハンドシェイクである。この認証方法は、公知であるため説明は省略する。また、認証時には、公開鍵配送法により、共有の秘密鍵（以下、「共有秘密鍵」という。）を生成し、生成した共有秘密鍵を用いて、情報の暗号化及び復号を行う。

認証が成功した場合には、コンテンツサーバ1001は、コンテンツ鍵の配信要求元へコンテンツ鍵を配信し、配信可能なコンテンツ鍵の数を1減算する。このとき、コンテンツサーバ1001は、再生装置1004へコンテンツ鍵の配信を行う場合には、コンテンツ鍵IDとコンテンツ鍵と対応情報IDとからなる第1鍵情報を配信し、再生装置1004には、第1鍵情報が格納される。ここで、コンテンツ鍵IDとは、コンテンツ鍵を識別する識別子であり、対応情報IDとは、コンテンツ鍵を用いて暗号化された暗号化コンテンツに対応する情報IDである。また、記録媒体1002へコンテンツ鍵の配信を行う場合には、コンテンツ鍵IDとコンテンツ鍵と対応情報IDと利用期限とからなる第2鍵情報を配信し、記録媒体1002には、第2鍵情報が格納される。ここで、利用期限とは、コンテンツ鍵の利用可能な期間を示す情報であり、日時を用いて記録されている。なお、コンテンツ鍵ID、コンテンツ鍵及び対応情報IDは、上記と同様であるため、説明は省略する。

【0106】

なお、鍵配信システム1000外にあるインターネット上の再生装置1005から、コンテンツサーバ1001は、コンテンツ鍵の配信要求を受け付け、再生装置1005と認証を行うが、失敗する。なぜなら、再生装置1005は、認証部を有している場合には、鍵配信システム1000内のみに有効な共通秘密情報を保持していないため、コンテンツサーバ1001との認証は、常に失敗することとなり、認証部を有していない場合も同様に、コンテンツサーバ1001との認証ができないため、常に失敗することとなる。また、鍵配信システム1000内のみに有効な共通秘密情報を保持していない記録媒体も同様にコンテンツサーバ1001との認証は失敗する。

【0107】

コンテンツサーバ1001は、コンテンツ鍵の利用が終了した旨の情報を受け取ると、配信可能なコンテンツ鍵の数を1加算する。

再生装置1004は、コンテンツサーバ1001にて暗号化された暗号化コンテンツを記憶しており、記憶している暗号化コンテンツを利用する場合には、コンテンツサーバ1001へコンテンツ鍵の配信要求を行い、コンテンツサーバ1001との認証後、認証が成功した場合に、コンテンツサーバ1001より第1鍵情報を取得し、取得した第1鍵情報に含まれるコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。再生終了後、再生装置1004は、使用した第1鍵情報を消去し、コンテンツ鍵の利用が終了した旨の情報をコンテンツサーバ1001へ送信する。

【0108】

記録媒体1002は、ICを内蔵している可搬型の記録媒体であり、例えば、ICを内蔵しているメモリカードである。記録媒体1002は、コンテンツサーバ1001にて暗号化された暗号化コンテンツを記憶している。記憶している暗号化コンテンツを利用する場合には、記録媒体1002は、再生装置1003へ装着される。再生装置1003は、暗号化コンテンツの利用時に、記録媒体1002に利用する暗号化コンテンツに対応する第2鍵情報が存在するか否かの判断を行い、存在する場合には、その第2鍵情報に含まれる利用期限を過ぎているか否かの判断を行い、過ぎていると判断する場合には、再生を行わず、利用期限内であると判断する場合には、その第2鍵情報に含まれるコンテンツ鍵を用いて、利用する暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【0109】

記録媒体 1002 に利用する暗号化コンテンツに対応する第 2 鍵情報が存在しないと判断する場合には、コンテンツサーバ 1001 へコンテンツ鍵の配信要求を行い、コンテンツサーバ 1001 と記録媒体 1002 との認証が行われた後、認証が成功した場合に、コンテンツサーバ 1001 より第 2 鍵情報を取得し、取得した第 2 鍵情報を記録媒体 1002 へ格納する。再生装置 1003 は、記録媒体 1002 へ格納した第 2 鍵情報に含まれるコンテンツ鍵を用いて、利用する暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

#### 【0110】

また、コンテンツサーバ 1001 は、再生装置 1003 と同様の動作にて、記録媒体 1002 に記憶されている暗号化コンテンツを利用することができる。さらに、コンテンツサーバ 1001 にて記憶している暗号化コンテンツを利用することもできる。この場合、コンテンツ鍵を取得する際の、認証は行わない。

10

このように、鍵配信システム 1000 は、コンテンツサーバ 1001 にて、コンテンツ鍵を管理し、鍵配信システム 1000 内にコンテンツ鍵の利用を制限、つまり、コンテンツの利用を制限したシステムである。

### 3. 2 コンテンツサーバ 1001 の構成

ここでは、コンテンツサーバ 1001 の構成について、説明する。

#### 【0111】

コンテンツサーバ 1001 は、図 17 に示すように、コンテンツ記憶部 1011、管理情報記憶部 1012、利用鍵記憶部 1013、受信部 1014、コンテンツ取得部 1015、入力部 1016、再生部 1017、利用鍵監視部 1018、利用鍵確認部 1019、利用鍵事前配信部 1020、コンテンツ鍵制御部 1021、認証部 1022、時間管理部 1023、入出力部 1024、通信部 1025 及び時計部 1026 から構成されている。

20

#### 【0112】

コンテンツサーバ 1001 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ネットワークインターフェースなどから構成されるコンピュータシステムである。前記 ROM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、コンテンツサーバ 1001 は、その機能を達成する。

#### 【0113】

30

##### (1) コンテンツ記憶部 1011

コンテンツ記憶部 1011 は、図 18 に一例として示すように、情報 ID と暗号化コンテンツを対応付けて記憶するための領域を備えている。

##### (2) 管理情報記憶部 1012

管理情報記憶部 1012 は、耐タンパ性を有しており、図 19 に示すように、鍵情報記憶部 1031 と、配信鍵情報記憶部 1032 とを備えている。

#### 【0114】

鍵情報記憶部 1031 は、図 20 に一例として示すように鍵情報テーブル T1001 を有している。鍵情報テーブル T1001 は、コンテンツ鍵 ID、コンテンツ鍵、対応情報 ID、総数、残数及び制限時間からなる組を 1 個以上記憶するための領域を備えている。なお、コンテンツ鍵 ID、コンテンツ鍵、対応情報 ID、総数、残数及び制限時間からなる情報をコンテンツ鍵情報と呼ぶ。

40

#### 【0115】

コンテンツ鍵 ID は、コンテンツ鍵を識別する識別子である。

コンテンツ鍵は、コンテンツの暗号化に使用した鍵であり、コンテンツ毎に異なる。

対応情報 ID は、コンテンツ鍵を用いて暗号化された暗号化コンテンツに対応する情報 ID である。これにより、コンテンツ記憶部 1011 に記憶されている暗号化コンテンツと、コンテンツ鍵との対応付けが可能となる。

#### 【0116】

総数は、配信可能なコンテンツ鍵と配信されたコンテンツ鍵の和であり、残数は、配信

50

可能なコンテンツ鍵の数である。

制限時間は、配信されたコンテンツ鍵が利用できる時間が記録されている。記録される時間の単位は、時単位であってもよいし、分単位、秒単位、日単位若しくはこれらの組合せであってもよい。ここでは、時単位で記録されている。

【0117】

配信鍵情報記憶部1032は、図21に一例として示すように、配信鍵情報テーブルT1002を有している。

配信鍵情報テーブルT1002は、配信コンテンツ鍵IDと利用期限とからなる組を1個以上記憶するための領域を備えている。なお、配信コンテンツ鍵IDと利用期限とからなる情報をコンテンツ鍵管理情報と呼ぶ。

10

【0118】

配信コンテンツ鍵IDは、記録媒体1002へ配信したコンテンツ鍵に対応するコンテンツ鍵IDである。

利用期限は、配信されたコンテンツ鍵が利用可能な期限を示し、日時分で記録される。なお、利用期限は、日時分秒であってもよい。

(3) 利用鍵記憶部1013

利用鍵記憶部1013は、耐タンパ性を有しており、コンテンツサーバ1001にて、利用中の暗号化コンテンツを復号し、コンテンツを生成するコンテンツ鍵を記憶している。

【0119】

20

(4) 時計部1026

時計部1026は、日時の計時を行う。

(5) 受信部1014

受信部1014は、放送局1006より、放送用に暗号化されたコンテンツを受信し、受信した暗号化されたコンテンツをコンテンツ取得部1015へ出力する。

【0120】

(6) コンテンツ取得部1015

コンテンツ取得部1015は、放送用に暗号化されたコンテンツを復号するための復号鍵と、鍵配信システム1000へ配信可能なコンテンツ鍵の総数及び制限時間を予め記憶している。

30

コンテンツ取得部1015は、受信部1014より、放送用に暗号化されたコンテンツを受け取ると、予め記憶している復号鍵を用いて、放送用に暗号化されたコンテンツを復号し、コンテンツを生成する。次に、乱数を用いて、コンテンツ鍵を生成し、生成したコンテンツ鍵を用いて、生成したコンテンツを暗号化し、暗号化コンテンツを生成する。生成した暗号化コンテンツを識別する情報IDを算出し、算出した情報IDと暗号化コンテンツとをコンテンツ記憶部1011へ格納する。

【0121】

さらに、コンテンツ取得部1015は、生成したコンテンツ鍵を識別するコンテンツ鍵IDを算出し、算出したコンテンツ鍵ID、情報IDと、生成したコンテンツ鍵と、予め記憶している総数、制限時間とを用いて、コンテンツ鍵情報を生成し、生成したコンテンツ鍵情報を鍵情報テーブルT1001へ書き込む。このとき、残数は、総数と同じ数である。

40

【0122】

(7) 入力部1016

入力部1016は、コンテンツ利用に係る情報を受け付け、受け付けた情報を再生部1017又は利用鍵事前配信部1020へ出力する。

入力部1016は、利用者より、利用する暗号化コンテンツの格納先が記録媒体1002であるか否かを示すコンテンツ格納先情報と、利用する暗号化コンテンツに対応する情報IDとを含む再生情報を受け付け、受け付けた再生情報を再生部1017へ出力する。

ここでは、コンテンツ格納先情報として、「0」、「1」を用いる。「0」の場合には、

50



利用する暗号化コンテンツの格納先は、記録媒体1002であることを示す。また、「1」の場合には、それ以外であることを示し、この場合では、利用する暗号化コンテンツの格納先は、コンテンツサーバ1001であることを示す。

【0123】

入力部1016は、利用者より、コンテンツの再生を中止する旨を示す再生中止情報を受け付けると、受け付けた再生中止情報を再生部1017へ出力する。

また、入力部1016は、利用者より、記録媒体1002へ事前にコンテンツ鍵の配信を要求する旨の事前要求情報を受け付け、受け付けた事前要求情報を利用鍵確認部1019へ出力する。ここで、事前要求情報とは、事前に配信を要求するコンテンツ鍵に対応する暗号化コンテンツの情報IDを含む情報である。

【0124】

(8) 再生部1017

再生部1017は、コンテンツ記憶部1011に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生、又は記録媒体1002に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【0125】

再生部1017は、入力部1016より再生情報を受け取り、受け取った再生情報に含まれるコンテンツ格納先情報を用いて、利用する暗号化コンテンツの格納先が記録媒体1002であるか否かの判断を行う。

利用する暗号化コンテンツの格納先が記録媒体1002であると判断する場合には、受け取った再生情報を利用鍵確認部1019へ出力する。

【0126】

利用する暗号化コンテンツの格納先が記録媒体1002以外、つまり、コンテンツサーバ1001であると判断する場合には、利用鍵監視部1018へ、受け取った再生情報を出力する。

再生部1017は、利用鍵監視部1018又は利用鍵確認部1019より、コンテンツ鍵の格納先が記録媒体1002であるか否かを示す鍵格納先情報を含む鍵取得完了情報を受け取る。ここでは、鍵格納先情報として、「0」、「1」を用いる。「0」の場合には、コンテンツ鍵の格納先は、記録媒体1002であることを示す。また、「1」の場合には、それ以外であることを示す。再生部1017が受け取った鍵取得完了情報に含まれる鍵格納先情報が「1」である場合には、コンテンツ鍵の格納先は、コンテンツサーバ1001であることを示す。

【0127】

受け取った鍵取得完了情報に含まれる鍵格納先情報を用いて、コンテンツ鍵の格納先が記録媒体1002であるか否かの判断を行う。

コンテンツ鍵の格納先が記録媒体1002であると判断する場合には、コンテンツ鍵を記録媒体1002より入出力部1024を介して取得し、さらには、入力部1016より受け取った再生情報に含まれる情報IDと対応する暗号化コンテンツを記録媒体1002より入出力部1024を介して取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【0128】

コンテンツ鍵の格納先が記録媒体1002以外、つまり、コンテンツサーバ1001であると判断する場合には、利用鍵記憶部1013に記憶している第1鍵情報に含まれるコンテンツ鍵を取得し、さらには、入力部1016より受け取った再生情報に含まれる情報IDと対応する暗号化コンテンツをコンテンツ記憶部1011から取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【0129】

また、再生部1017は、入力部1016より再生中止情報を受け取ると、再生中のコ

10

20

30

40

50

ンテンツの再生を中止する。

( 9 ) 利用鍵監視部 1018

利用鍵監視部 1018 は、再生部 1017 にて、コンテンツ記憶部 1011 に記憶している暗号化コンテンツを使用する際に利用する第 1 鍵情報を利用鍵記憶部 1013 へ格納し、暗号化コンテンツの利用終了時には、格納した第 1 鍵情報の消去を行う。

【 0130 】

利用鍵監視部 1018 は、再生部 1017 より再生情報を受け取ると、第 1 要求情報を生成し、生成した第 1 要求情報をコンテンツ鍵制御部 1021 へ出力する。ここで、第 1 要求情報とは、コンテンツ鍵を利用鍵記憶部 1013 へ格納する旨の情報であり、再生情報に含まれている情報 ID を含んでいる。

10

利用鍵監視部 1018 は、コンテンツ鍵制御部 1021 より、第 1 鍵情報を受け取り、受け取った第 1 鍵情報を利用鍵記憶部 1013 へ格納し、鍵格納先情報が「 1 」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部 1017 へ出力する。

【 0131 】

さらに、利用鍵監視部 1018 は、再生部 1017 の動作の監視を行い、コンテンツの再生終了若しくは、コンテンツ再生中止により再生部 1017 の動作が終了したこと、つまりコンテンツの利用が終了したことを検知すると、利用鍵記憶部 1013 に記憶している第 1 鍵情報を消去し、コンテンツ鍵の利用が終了したことを示す鍵利用終了情報を生成し、生成した鍵利用終了情報をコンテンツ鍵制御部 1021 へ出力する。ここで、鍵利用終了情報は、利用した暗号化コンテンツに対応する情報 ID を含んでいる。

20

【 0132 】

( 10 ) 利用鍵確認部 1019

利用鍵確認部 1019 は、記録媒体 1002 に記録されているコンテンツ鍵の利用期間の確認及びコンテンツ鍵の記録及び消去を行う。

利用鍵確認部 1019 は、再生部 1017 より再生情報を受け取ると、受け取った再生情報に含まれる情報 ID と対応する第 2 鍵情報が存在するか否かの判断を行う。

【 0133 】

第 2 鍵情報が存在すると判断する場合には、時計部 1026 より、現在の日時を取得し、存在する第 2 鍵情報に含まれるコンテンツ鍵の利用期限が過ぎているか否かの判断を行う。利用期限内であると判断する場合には、鍵格納先情報が「 0 」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部 1017 へ出力し、利用期限を過ぎていると判断する場合には、第 2 鍵情報を消去し、コンテンツ鍵の利用不可を示す利用不可情報を利用者へ通知する。

30

【 0134 】

第 2 鍵情報が存在しないと判断する場合には、第 2 要求情報を生成し、生成した第 2 要求情報をコンテンツ鍵制御部 1021 へ出力する。また、再生情報を受け取った旨の情報を入出力部 1024 を介して記録媒体 1002 へ出力する。ここで、第 2 要求情報とは、コンテンツ鍵を記録媒体 1002 へ出力する旨の情報であり、再生情報に含まれている情報 ID を含んでいる。

【 0135 】

40

利用鍵確認部 1019 は、コンテンツ鍵制御部 1021 より、暗号化された第 2 鍵情報を受け取り、受け取った暗号化された第 2 鍵情報を入出力部 1024 を介して記録媒体 1002 へ出力する。さらに、利用鍵確認部 1019 は、鍵格納先情報が「 0 」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部 1017 へ出力する。

( 11 ) 利用鍵事前配信部 1020

利用鍵事前配信部 1020 は、記録媒体 1002 へ、コンテンツ鍵の事前配信を行う。

【 0136 】

利用鍵事前配信部 1020 は、事前要求情報を受け取ると、受け取った事前要求情報をコンテンツ鍵制御部 1021 へ出力し、さらに、事前要求情報を受け取った旨の情報を入出力部 1024 を介して記録媒体 1002 へ出力する。

50

利用鍵事前配信部 1020 は、コンテンツ鍵制御部 1021 より、暗号化された第 2 鍵情報を受け取り、受け取った暗号化された第 2 鍵情報を入出力部 1024 を介して記録媒体 1002 へ出力する。

【0137】

(12) コンテンツ鍵制御部 1021

コンテンツ鍵制御部 1021 は、配信するコンテンツ鍵の管理を行う。

コンテンツ鍵制御部 1021 は、第 1 要求情報、第 2 要求情報、コンテンツ鍵の配信をネットワークを利用して行う旨の第 3 要求情報、又は事前要求情報を受け付ける。さらに、コンテンツ鍵制御部 1021 は、鍵利用終了情報を利用鍵監視部 1018 又は、通信部 1025 を介して再生装置 1004 より受け付ける。

10

【0138】

ここで、第 3 要求情報は、利用種別と利用する暗号化コンテンツに対応する情報 ID とを含んでいる。また、利用種別には、再生装置を示す情報又は記録媒体を示す情報の何れかが記録されている。利用種別として、再生装置を示す情報が記録されている場合には、利用するコンテンツは再生装置に記憶されていることを示し、記録媒体を示す情報が記録されている場合には、利用するコンテンツは記録媒体に記憶されていることを示す。なお、コンテンツ鍵制御部 1021 は、再生装置 1005 からの第 3 要求情報をも受け付ける。

【0139】

コンテンツ鍵制御部 1021 は、受け付けた情報が、鍵利用終了情報であるか否かを判断する。

20

鍵利用終了情報でないと判断する場合には、さらに、第 1 要求情報であるか否かを判断する。

第 1 要求情報であると判断する場合には、第 1 要求情報に含まれる情報 ID を用いて、情報 ID と一致する対応情報 ID を含むコンテンツ鍵情報を鍵情報テーブル T1001 より取得する。取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する。「0」であると判断する場合には、コンテンツ鍵の残数が「0」である旨の残数無情報を利用者へ通知する。「0」でないと判断する場合には、取得したコンテンツ鍵情報より第 1 鍵情報を生成し、生成した第 1 鍵情報を利用鍵監視部 1018 へ出力する。さらに、コンテンツ鍵制御部 1021 は、取得したコンテンツ鍵情報の残数を 1 減算して、取得したコンテンツ鍵情報を更新して、鍵情報テーブル T1001 へ書き込む。

30

【0140】

第 1 要求情報でないと判断する場合には、受け付けた情報が第 2 要求情報、利用種別が再生装置である第 3 要求情報、利用種別が記録媒体である第 3 要求情報、又は事前要求情報の何れかであることを示す認証識別情報を認証部 1022 へ出力する。

コンテンツ鍵制御部 1021 は、認証部 1022 から認証が成功した旨の認証成功情報を受け取ると、以下のようにして、コンテンツ鍵の取得、配信及び鍵情報テーブル T1001 の更新を行う。

【0141】

コンテンツ鍵制御部 1021 は、受け付けた情報が、第 2 要求情報、第 3 要求情報、又は事前要求情報の何れかであるかの判断を行う。

40

第 2 要求情報であると判断する場合には、第 2 要求情報に含まれる情報 ID を用いて、第 1 要求情報の場合と同様に、コンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する。「0」であると判断する場合には、コンテンツ鍵の残数が「0」である旨の残数無情報を利用者へ通知する。「0」でないと判断する場合には、さらに、時計部 1026 より現在の日時を取得し、取得した日時とコンテンツ鍵情報に含まれる制限時間とを用いて、利用期限を算出する。算出した利用期限及び取得したコンテンツ鍵情報より第 2 鍵情報を生成し、生成した第 2 鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第 2 鍵情報を利用鍵確認部 1019 へ出力する。さらに、コンテンツ鍵制御部 1021 は、取得したコンテンツ鍵情報の残数を 1 減算し

50

て、取得したコンテンツ鍵情報を更新して、鍵情報テーブルT1001へ書き込む。また、コンテンツ鍵制御部1021は、算出した利用期限及び取得したコンテンツ鍵情報よりコンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルT1002に書き込む。

#### 【0142】

第3要求情報であると判断する場合には、第3要求情報に含まれる情報IDを用いて、第1要求情報の場合と同様に、コンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する。「0」であると判断する場合には、コンテンツ鍵の残数が「0」である旨の残数無情報を利用者へ通知する。「0」でないと判断する場合には、さらに、第3要求情報に含まれる利用種別が再生装置を示すか又は記録媒体を示すかの判断を行う。

10

#### 【0143】

利用種別が再生装置を示すと判断する場合には、第1鍵情報を生成し、生成した第1鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第1鍵情報を通信部1025を介して再生装置1004へ出力する。さらに、コンテンツ鍵制御部1021は、取得したコンテンツ鍵情報の残数を1減算して、取得したコンテンツ鍵情報を更新して、鍵情報テーブルT1001へ書き込む。

#### 【0144】

利用種別が記録媒体を示すと判断する場合には、さらに、時計部1026より現在の日時を取得し、取得した日時とコンテンツ鍵情報に含まれる制限時間とを用いて、利用期限を算出し、算出した利用期限及び取得したコンテンツ鍵情報より第2鍵情報を生成し、生成した第2鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第2鍵情報を通信部1025を介して再生装置1003に装着された記録媒体1002へ送信する。さらに、コンテンツ鍵制御部1021は、取得したコンテンツ鍵情報の残数を1減算して、取得したコンテンツ鍵情報を更新して、鍵情報テーブルT1001へ書き込む。また、コンテンツ鍵制御部1021は、算出した利用期限及び取得したコンテンツ鍵情報よりコンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルT1002に書き込む。

20

#### 【0145】

事前要求情報であると判断する場合には、事前要求情報に含まれる情報IDを用いて、情報IDと一致する対応情報IDを含むコンテンツ鍵情報を鍵情報テーブルT1001より取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する。「0」であると判断する場合には、コンテンツ鍵の残数が「0」である旨の残数無情報を利用者へ通知する。「0」でないと判断する場合には、さらに、時計部1026より現在の日時を取得し、取得した日時とコンテンツ鍵情報に含まれる制限時間とを用いて、利用期限を算出し、算出した利用期限及び取得したコンテンツ鍵情報より第2鍵情報を生成し、生成した第2鍵情報を、認証時に生成された共有秘密鍵を用いて暗号化し、暗号化した第2鍵情報を利用鍵事前配信部1020へ出力する。さらに、コンテンツ鍵制御部1021は、取得したコンテンツ鍵情報の残数を1減算して、取得した第2鍵情報を更新して、鍵情報テーブルT1001へ書き込む。また、コンテンツ鍵制御部1021は、算出した利用期限及び取得したコンテンツ鍵情報よりコンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルT1002に書き込む。

30

40

#### 【0146】

コンテンツ鍵制御部1021は、受け付けた情報が、鍵利用終了情報であると判断する場合には、受け付けた鍵利用終了情報に含まれる情報IDを用いて、情報IDと一致する対応情報IDを含むコンテンツ鍵情報を鍵情報テーブルT1001より取得する。取得したコンテンツ鍵情報の残数を1加算して、取得したコンテンツ鍵情報を更新し、鍵情報テーブルT1001へ書き込む。

#### 【0147】

(13) 認証部1022

50

認証部 1022 は、予め共通秘密情報を記憶しており、この共通秘密情報を用いて、コンテンツサーバ 1001 に装着された記録媒体 1002 との認証、再生装置 1004 との認証、又は再生装置 1003 に装着された記録媒体 1002 との認証を行う。

認証部 1022 は、コンテンツ鍵制御部 1021 より認証識別情報を受け取ると、受け取った認証指示情報を用いて、以下のようにして、認証を行う。

【0148】

認証識別情報が、第 2 要求情報又は事前要求情報を示すと判断する場合には、コンテンツサーバ 1001 に装着された記録媒体 1002 と互いに認証を行う。

利用種別が再生装置である第 3 要求情報を示すと判断する場合には、再生装置 1004 と互いに認証を行い、利用種別が記録媒体である第 3 要求情報を示すと判断する場合には、再生装置 1003 に装着された記録媒体 1002 と互いに認証を行う。

【0149】

なお、認証部 1022 は、認証開始時に、共有秘密鍵を生成し、生成した共有秘密鍵を用いて、認証に利用する情報を暗号化し、暗号化した情報を再生装置 1004 又は記録媒体 1002 へ送信し、また、再生装置 1004 又は記録媒体 1002 から暗号化された情報を受け取り、受け取った暗号化された情報を復号して、復号した情報を認証に利用する。

【0150】

認証部 1022 は、認証が成功したか否かの判断を行い、認証が成功した場合には、認証成功情報をコンテンツ鍵制御部 1021 へ出力し、認証が失敗した場合には、認証が失敗した旨の認証失敗情報を利用者へ通知する。

(14) 時間管理部 1023

時間管理部 1023 は、時計部 1026 を用いて、配信鍵情報テーブル T1002 に記録されている配信コンテンツ鍵 ID に対応する利用期限を管理する。

【0151】

時間管理部 1023 は、時計部 1026 を用いて、配信鍵情報テーブル T1002 に記録されている配信コンテンツ鍵 ID に対応する利用期限が過ぎているか否かの判断を行う。利用期限が過ぎていると判断する場合には、そのコンテンツ鍵管理情報を削除し、削除した配信コンテンツ鍵 ID と一致するコンテンツ鍵情報を鍵情報テーブル T1001 より取得し、取得したコンテンツ鍵情報に含まれる残数に 1 加算し、コンテンツ鍵情報を更新し、鍵情報テーブル T1001 へ書き込む。

【0152】

(15) 入出力部 1024

入出力部 1024 は、コンテンツサーバ 1001 に装着された記録媒体 1002 より情報を受け取り、受け取った情報を再生部 1017、利用鍵確認部 1019、利用鍵事前配信部 1020 又は認証部 1022 へ出力する。

また、入出力部 1024 は、再生部 1017、利用鍵確認部 1019、利用鍵事前配信部 1020 又は認証部 1022 より受け取った情報をコンテンツサーバ 1001 に装着された記録媒体 1002 へ出力する。

【0153】

(16) 通信部 1025

通信部 1025 は、コンテンツ鍵制御部 1021 より受け取った情報を再生装置 1004 又は、再生装置 1003 に装着された記録媒体 1002 へ送信し、認証部 1022 より受け取った情報を再生装置 1004、再生装置 1003 に装着された記録媒体 1002 又は再生装置 1005 へ送信する。

【0154】

また、通信部 1025 は、再生装置 1004、再生装置 1003 に装着された記録媒体 1002 又は再生装置 1005 より受け取った情報をコンテンツ鍵制御部 1021 又は認証部 1022 へ出力する。

3. 3 記録媒体 1002 の構成

10

20

30

40

50

ここでは、記録媒体1002の構成について、説明する。

【0155】

記録媒体1002は、図22に示すように、コンテンツ記憶部1101、利用鍵記憶部1102、認証部1103、及び入出力部1104から構成されている。

記録媒体1002は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、記録媒体1002は、その機能を達成する。

【0156】

(1) コンテンツ記憶部1101

コンテンツ記憶部1101は、コンテンツサーバ1001が備えるコンテンツ記憶部1011と同様の領域を備えている。

(2) 利用鍵記憶部1102

利用鍵記憶部1102は、耐タンパ性を有しており、図23に一例として示すように、第2鍵情報を1以上記憶するための配信コンテンツ鍵テーブルT1101を備えている。

【0157】

配信コンテンツ鍵テーブルT1101の各項目については、第2鍵情報を構成するデータと同様であるため、説明は省略する。

(3) 認証部1103

認証部1103は、予め共通秘密情報を記憶しており、コンテンツサーバ1001が備える認証部1022と認証を行う。

【0158】

認証部1103は、再生情報又は事前要求情報を受け取った旨の情報を入出力部1104を介してコンテンツサーバ1001から受け取ることにより、又は再生装置1003が再生情報を受け取った旨の情報を入出力部1104を介して再生装置1003から受け取ることにより、コンテンツサーバ1001と互いに認証を行う。

認証部1103は、認証が成功したか否かの判断を行い、認証が成功した場合には、認証成功情報を入出力部1104を介して再生装置1003へ出力し、認証が失敗した場合には、認証失敗情報を利用者へ通知する。

【0159】

また、認証部1103は、コンテンツサーバ1001の認証部1022と同様に、認証開始時に、共有秘密鍵を生成する。生成した共有秘密鍵を用いて、認証に利用する情報を暗号化し、暗号化した情報をコンテンツサーバ1001へ送信し、また、コンテンツサーバ1001から暗号化された情報を受け取り、受け取った暗号化された情報を復号して、復号した情報を認証に利用する。

【0160】

(4) 入出力部1104

入出力部1104は、記録媒体1002が装着された装置より情報を受け取る。入出力部1104は、受け取った情報が、認証に係る情報であるか、暗号化コンテンツであるか又は暗号化された第2鍵情報であるかの判断を行う。

認証に係る情報であると判断する場合には、認証部1103へ出力し、暗号化されたコンテンツであると判断する場合には、コンテンツ記憶部1101へ書き込む。暗号化された第2鍵情報であると判断する場合には、認証時に生成された共有秘密鍵を用いて暗号化された第2鍵情報を復号して、第2鍵情報を生成し、生成した第2鍵情報を、利用鍵記憶部1102へ書き込む。

【0161】

また、入出力部1104は、コンテンツ記憶部1101、利用鍵記憶部1102、又は認証部1103より受け取った情報を、記録媒体1002が装着された装置へ出力する。

3.4 再生装置1003の構成

10

20

30

40

50

ここでは、再生装置 1003 の構成について、説明する。

【0162】

再生装置 1003 は、図 24 に示すように、入力部 1201、再生部 1202、利用鍵確認部 1203、入出力部 1204、通信部 1205 及び時計部 1206 から構成されている。

再生装置 1003 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ネットワークインターフェースなどから構成されるコンピュータシステムである。前記 ROM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置 1003 は、その機能を達成する。

10

【0163】

(1) 時計部 1206

時計部 1206 は、日時の計時を行う。

(2) 入力部 1201

入力部 1201 は、コンテンツ利用に係る情報を受け付け、受け付けた情報を再生部 1202 へ出力する。

【0164】

入力部 1201 は、利用者より、再生情報を受け付け、受け付けた再生情報を再生部 1202 へ出力する。ここで、再生情報に含まれるコンテンツ格納先情報は、常に「0」である。

20

入力部 1201 は、利用者より、コンテンツの再生を中止する旨を示す再生中止情報を受け付けると、受け付けた再生中止情報を再生部 1202 へ出力する。

【0165】

(3) 再生部 1202

再生部 1202 は、記録媒体 1002 に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

再生部 1202 は、入力部 1201 より再生情報を受け取ると、受け取った再生情報を利用鍵確認部 1203 へ出力する。

【0166】

再生部 1202 は、利用鍵確認部 1203 より、鍵取得完了情報を受け取ると、記録媒体 1002 よりコンテンツ鍵を取得し、さらには、入力部 1201 より受け取った再生情報に含まれる情報 ID と対応する暗号化コンテンツを記録媒体 1002 のコンテンツ記憶部 1101 から取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

30

【0167】

また、再生部 1202 は、入力部 1201 より再生中止情報を受け取ると、再生中のコンテンツの再生を中止する。

(4) 利用鍵確認部 1203

利用鍵確認部 1203 は、記録媒体 1002 に記録されているコンテンツ鍵の利用期間の確認及びコンテンツ鍵の記録及び消去を行う。

40

【0168】

利用鍵確認部 1203 は、再生部 1202 より再生情報を受け取ると、受け取った再生情報に含まれる情報 ID と対応する第 2 鍵情報が記録媒体 1002 に存在するか否かの判断を行う。

第 2 鍵情報が存在すると判断する場合には、時計部 1206 より、現在の日時を取得し、存在する第 2 鍵情報に含まれるコンテンツ鍵の利用期限が過ぎているか否かの判断を行う。利用期限内であると判断する場合には、鍵格納先情報が「0」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部 1202 へ出力する。利用期限を過ぎていると判断する場合には、第 2 鍵情報を消去し、コンテンツ鍵の利用不可を示す利用不可情報を利用者へ通知する。

50

## 【0169】

第2鍵情報が存在しないと判断する場合には、記録媒体を示す情報が記録された利用種別と、受け取った再生情報に含まれる情報IDとを含む第3要求情報を生成し、生成した第3要求情報をコンテンツサーバ1001へ出力する。また、再生情報を受け取った旨の情報を入出力部1024を介して記録媒体1002へ出力する。

利用鍵確認部1203は、認証部1103より入出力部1204を介して、認証成功情報を受け取ると、さらに、通信部1205を介してコンテンツサーバ1001より、暗号化された第2鍵情報を受け取り、受け取った暗号化された第2鍵情報を入出力部1204を介して記録媒体1002へ出力する。さらに、利用鍵確認部1203は、鍵格納先情報が「0」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部1202へ出力する。

10

## 【0170】

## (5) 入出力部1204

入出力部1204は、記録媒体1002より受け取った情報を、再生部1202、利用鍵確認部1203又は通信部1205へ出力する。

また、入出力部1204は、再生部1202、利用鍵確認部1203又は通信部1205から受け取った情報を記録媒体1002へ出力する。

## 【0171】

## (6) 通信部1205

通信部1205は、コンテンツサーバ1001より受け取った情報を利用鍵確認部1203又は入出力部1204へ出力する。

20

また、通信部1205は、利用鍵確認部1203又は入出力部1204より受け取った情報をコンテンツサーバ1001へ送信する。

## 3.5 再生装置1004の構成

ここでは、再生装置1004の構成について、説明する。

## 【0172】

再生装置1004は、図25に示すように、コンテンツ記憶部1301、利用鍵記憶部1302、入力部1303、再生部1304、利用鍵監視部1305、認証部1306及び通信部1307から構成されている。

再生装置1004は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ネットワークインターフェースなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、再生装置1004は、その機能を達成する。

30

## 【0173】

## (1) コンテンツ記憶部1301

コンテンツ記憶部1301は、コンテンツサーバ1001が備えるコンテンツ記憶部1011と同様の領域を備えている。

## (2) 利用鍵記憶部1302

利用鍵記憶部1302は、耐タンパ性を有しており、再生装置1004にて利用中の暗号化コンテンツを復号し、コンテンツを生成するコンテンツ鍵を記憶している。

40

## 【0174】

## (3) 入力部1303

入力部1303は、コンテンツ利用に係る情報を受け付け、受け付けた情報を再生部1304へ出力する。

入力部1303は、利用者より、再生情報を受け付け、受け付けた再生情報を再生部1304へ出力する。ここで、再生情報に含まれるコンテンツ格納先情報は、常に「1」である。

## 【0175】

入力部1303は、利用者より、コンテンツの再生を中止する旨を示す再生中止情報を

50



受け付けると、受け付けた再生中止情報を再生部 1304 へ出力する。

(4) 再生部 1304

再生部 1304 は、コンテンツ記憶部 1301 に記憶されている暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツの再生を行う。

【0176】

再生部 1304 は、入力部 1303 より再生情報を受け取ると、受け取った再生情報を利用鍵監視部 1305 へ出力する。

再生部 1304 は、利用鍵監視部 1305 より、鍵取得完了情報を受け取ると、利用鍵記憶部 1302 より第 1 鍵情報に含まれるコンテンツ鍵を取得し、さらには、入力部 1303 より受け取った再生情報に含まれる情報 ID と対応する暗号化コンテンツをコンテンツ記憶部 1301 から取得し、取得したコンテンツ鍵を用いて、暗号化コンテンツを復号して、コンテンツを生成し、生成したコンテンツを再生する。

【0177】

また、再生部 1304 は、入力部 1303 より再生中止情報を受け取ると、再生中のコンテンツの再生を中止する。

(5) 利用鍵監視部 1305

利用鍵監視部 1305 は、再生部 1304 にてコンテンツ記憶部 1301 に記憶している暗号化コンテンツを使用する際に利用するコンテンツ鍵を利用鍵記憶部 1302 へ格納し、暗号化コンテンツの利用終了時には、格納したコンテンツ鍵の消去を行う。

【0178】

利用鍵監視部 1305 は、再生部 1304 より再生情報を受け取ると、再生装置を示す情報が記録された利用種別と、受け取った再生情報に含まれる情報 ID とを含む第 3 要求情報を生成し、生成した第 3 要求情報をコンテンツサーバ 1001 へ出力し、さらに、再生情報を受け取った旨の情報を認証部 1306 へ出力する。

利用鍵監視部 1305 は、認証部 1306 より認証成功情報を受け取ると、さらに、コンテンツサーバ 1001 より通信部 1307 を介して、暗号化された第 1 鍵情報を受け取る。利用鍵監視部 1305 は、認証時に生成された共有秘密鍵を用いて、受け取った暗号化された第 1 鍵情報を復号して、第 1 鍵情報を生成し、生成した第 1 鍵情報を利用鍵記憶部 1302 へ格納する。さらに、利用鍵監視部 1305 は、鍵格納先情報が「1」である鍵取得完了情報を生成し、生成した鍵取得完了情報を再生部 1304 へ出力する。この場合、鍵格納先情報が「1」である場合には、コンテンツ鍵の格納先は、再生装置 1004 の利用鍵記憶部 1302 であることを示す。

【0179】

さらに、利用鍵監視部 1305 は、再生部 1304 の動作の監視を行い、コンテンツの再生終了若しくは、コンテンツ再生中止により再生部 1304 の動作が終了したこと、つまりコンテンツの利用が終了したことを検知すると、利用鍵記憶部 1302 に記憶している第 1 鍵情報を消去し、鍵利用終了情報を生成し、生成した鍵利用終了情報をコンテンツサーバ 1001 へ出力する。

【0180】

(6) 認証部 1306

認証部 1306 は、予め共通秘密情報を記憶しており、コンテンツサーバ 1001 が備える認証部 1022 と認証を行う。

認証部 1306 は、利用鍵監視部 1305 より再生情報を受け取った旨の情報を受け取ることにより、コンテンツサーバ 1001 と互いに認証を行う。

【0181】

認証部 1306 は、認証が成功したか否かの判断を行い、認証が成功した場合には、認証成功情報を利用鍵監視部 1305 へ出力し、認証が失敗した場合には、認証が失敗した旨の認証失敗情報を利用者へ通知する。

また、認証部 1306 は、コンテンツサーバ 1001 の認証部 1022 と同様に、認証開始時に、共有秘密鍵を生成する。生成した共有秘密鍵を用いて、認証に利用する情報を

10

20

30

40

50

暗号化し、暗号化した情報をコンテンツサーバ1001へ送信し、また、コンテンツサーバ1001から暗号化された情報を受け取り、受け取った暗号化された情報を復号して、復号した情報を認証に利用する。

#### 【0182】

##### (7) 通信部1307

通信部1307は、コンテンツサーバ1001より受信した情報を利用鍵監視部1305又は認証部1306へ出力する。

また、通信部1307は、利用鍵監視部1305又は認証部1306より受け取った情報をコンテンツサーバ1001へ出力する。

#### 3.6 鍵配信システム1000の動作

ここでは、鍵配信システム1000の動作について、説明する。

#### 【0183】

##### (1) コンテンツ鍵管理処理

ここでは、コンテンツサーバ1001のコンテンツ鍵制御部1021と認証部1022とで行われるコンテンツ鍵管理処理について、図26及び図27の流れ図を用いて説明する。

コンテンツ鍵制御部1021は、情報を受け付け(ステップS1000)、受け付けた情報が、鍵利用終了情報であるか否かの判断を行う(ステップS1005)。

#### 【0184】

ステップS1005にて鍵利用終了情報であると判断する場合には、受け付けた鍵利用終了情報に含まれる情報IDを用いて、情報IDに対応するコンテンツ鍵情報の残数を1加算して、鍵情報テーブルT1001の更新を行う(ステップS1010)。

ステップS1005にて鍵利用終了情報でないと判断する場合には、受け付けた情報が、第1要求情報であるか否かを判断する(ステップS1015)。

#### 【0185】

ステップS1015にて第1要求情報であると判断する場合には、第1要求情報に含まれる情報IDに対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する(ステップS1020)。

ステップS1020にて残数が「0」でないと判断する場合には、取得したコンテンツ鍵情報より第1鍵情報を生成し、生成した第1鍵情報を利用鍵監視部1018へ出力する(ステップS1025)。さらに、取得したコンテンツ鍵情報の残数を1減算して、鍵情報テーブルT1001を更新する(ステップS1030)。

#### 【0186】

ステップS1020にて、残数が「0」であると判断する場合には、残数無情報を利用者へ通知する(ステップS1135)。

ステップS1015にて第1要求情報でないと判断する場合には、コンテンツ鍵制御部1021は、認証識別情報を認証部1022へ出力し、認証部1022にて、コンテンツ鍵の配信要求元と認証処理を行う(ステップS1035)。ステップS1035にて行われた認証処理が成功したか否かを判断する(ステップS1040)。ステップS1040にて認証が失敗と判断する場合には、認証失敗情報を利用者へ通知する(ステップS1045)。

#### 【0187】

ステップS1040にて認証が成功と判断する場合には、受け付けた情報が、第2要求情報であるか否かを判断する(ステップS1050)。

ステップS1050にて第2要求情報であると判断する場合には、第2要求情報に含まれる情報IDに対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する(ステップS1055)。

#### 【0188】

ステップS1055にて残数が「0」でないと判断する場合には、取得したコンテンツ鍵情報より第2鍵情報を生成し、生成した第2鍵情報を暗号化して、暗号化した第2鍵情

10

20

30

40

50

報を利用鍵確認部 1019 へ出力する（ステップ S1060）。さらに、取得したコンテンツ鍵情報の残数を 1 減算して、鍵情報テーブル T1001 を更新する（ステップ S1065）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブル T1002 に書き込む（ステップ S1070）。

【0189】

ステップ S1055 にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する（ステップ S1135）。

ステップ S1050 にて第 2 要求情報でないと判断する場合には、受け付けた情報が第 3 要求情報であるか否かを判断する（ステップ S1075）。

ステップ S1075 にて第 3 要求情報であると判断する場合には、第 3 要求情報に含まれる情報 ID に対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する（ステップ S1080）。 10

【0190】

ステップ S1080 にて残数が「0」でないと判断する場合には、受け付けた第 3 要求情報に含まれる利用種別が再生装置を示す情報であるか否かを判断する（ステップ S1085）。

ステップ S1085 にて再生装置を示す情報であると判断する場合には、取得したコンテンツ鍵情報より第 1 鍵情報を生成し、生成した第 1 鍵情報を暗号化して、暗号化した第 1 鍵情報を再生装置 1004 へ送信する（ステップ S1090）。さらに、取得したコンテンツ鍵情報の残数を 1 減算して、鍵情報テーブル T1001 を更新する（ステップ S1065）。 20

【0191】

ステップ S1085 にて再生装置を示す情報でないと判断する場合には、取得したコンテンツ鍵情報より第 2 鍵情報を生成し、生成した第 2 鍵情報を暗号化して、暗号化した第 2 鍵情報を記録媒体 1002 へ送信する（ステップ S1100）。さらに、取得したコンテンツ鍵情報の残数を 1 減算して、鍵情報テーブル T1001 を更新する（ステップ S1105）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブル T1002 に書き込む（ステップ S1110）。

【0192】

ステップ S1080 にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する（ステップ S1135）。 30

ステップ S1075 にて第 3 要求情報でないと判断する、つまり、受け付けた情報が事前要求情報であると判断する場合には、受け付けた事前要求情報に含まれる情報 ID に対応するコンテンツ鍵情報を取得し、取得したコンテンツ鍵情報の残数が「0」であるか否かを判断する（ステップ S1115）。

【0193】

ステップ S1115 にて残数が「0」でないと判断する場合には、取得したコンテンツ鍵情報より第 2 鍵情報を生成し、生成した第 2 鍵情報を暗号化して、暗号化した第 2 鍵情報を利用鍵事前配信部 1020 へ出力する（ステップ S1120）。さらに、取得したコンテンツ鍵情報の残数を 1 減算して、鍵情報テーブル T1001 を更新する（ステップ S1125）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブル T1002 に書き込む（ステップ S1130）。 40

【0194】

ステップ S1115 にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する（ステップ S1135）。

（2） 認証処理の動作

ここでは、コンテンツ鍵管理処理にて行われる認証処理について、図 28 の流れ図を用いて説明する。

【0195】

認証部 1022 は、コンテンツ鍵制御部 1021 より、認証識別情報を受け取ると、受 50

け取った認証識別情報が、第2要求情報又は事前要求情報を示すか否かを判断する（ステップS1150）。

第2要求情報又は事前要求情報を示すと判断する場合には、コンテンツサーバ1001に装着された記録媒体1002と、互いに認証を行う（ステップS1155）。

【0196】

ステップS1150にて、受け取った認証識別情報が、第2要求情報を示す情報でなく、且つ事前要求情報を示す情報でないと判断する場合には、利用種別が再生装置である第3要求情報であるか否かを判断する（ステップS1160）。

利用種別が再生装置である第3要求情報を示すと判断する場合には、再生装置1004と、互いに認証を行い（ステップS1165）、利用種別が再生装置である第3要求情報でないと判断する場合、つまり、利用種別が記録媒体である第3要求情報を示すと判断する場合には、再生装置1003に装着された記録媒体1002と、互いに認証を行う（ステップS1170）。

【0197】

### （3） 時間管理処理

ここでは、コンテンツサーバ1001の時間管理部1023にて行われる時間管理処理について、図29の流れ図を用いて説明する。

時間管理部1023は、配信鍵情報テーブルT1002よりコンテンツ鍵管理情報の取得と、時計部1026より現在の日時の取得を行い（ステップS1200）、取得した日時を用いて、コンテンツ鍵管理情報に含まれる利用期限を過ぎているか否かを判断する（ステップS1205）。

【0198】

ステップS1205にて利用期限が過ぎていると判断する場合には、取得したコンテンツ鍵管理情報を配信鍵情報テーブルT1002より削除し（ステップS1210）、取得したコンテンツ鍵管理情報の配信コンテンツ鍵IDと対応するコンテンツ鍵情報の残数を1加算して、鍵情報テーブルT1001の更新を行う（ステップS1215）。

なお、この処理を配信鍵情報テーブルT1002に記憶されているコンテンツ鍵管理情報の数分繰り返す。

【0199】

### （4） 再生装置1004における再生時の動作

ここでは、再生装置1004に記憶されている暗号化コンテンツを利用する場合の動作について、図30に示す流れ図を用いて説明する。

再生装置1004は、再生情報を受け付けると（ステップS1250）、再生装置を示す利用種別を含む第3要求情報を生成し、生成した第3要求情報をコンテンツサーバ1001へ送信する（ステップS1255）。

【0200】

コンテンツサーバ1001は、第3要求情報を受信すると（ステップS1260）、再生装置1004と互いに認証を行う（ステップS1265、ステップS1270）。

コンテンツサーバ1001は、再生装置1004との認証が成功したか否かの判断を行う（ステップS1275）。

コンテンツサーバ1001は、ステップS1275にて認証が成功したと判断する場合には、第3要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数が「0」であるか否かを判断する（ステップS1285）。ステップS1275にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップS1340）。

【0201】

コンテンツサーバ1001は、ステップS1285にて残数が「0」でないと判断する場合には、第1鍵情報を生成し、生成した第1鍵情報を暗号化して、再生装置1004へ送信する（ステップS1290）。ステップS1285にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する（ステップS1345）。

コンテンツサーバ1001は、第3要求情報に含まれる情報IDに対応するコンテンツ

10

20

30

40

50

鍵情報の残数を1減算して、鍵情報テーブルT1001を更新する(ステップS1295)。

#### 【0202】

再生装置1004は、認証が成功したか否かを判断する(ステップS1280)。

再生装置1004は、ステップS1280にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する(ステップS1335)。認証が成功したと判断する場合には、コンテンツサーバ1001より暗号化された第1鍵情報を受信し、暗号化された第1鍵情報を復号して、第1鍵情報を生成する(ステップS1300)。

#### 【0203】

再生装置1004は、生成した第1鍵情報を利用鍵記憶部1302へ格納し(ステップS1305)、格納した第1鍵情報と、コンテンツ記憶部1301に記憶されている暗号化コンテンツを用いて、コンテンツを再生する(ステップS1310)。また、コンテンツ利用終了を検知すると(ステップS1315)、利用鍵記憶部1302へ格納した第1鍵情報を消去し(ステップS1320)、鍵利用終了情報生成し、生成した鍵終了情報をコンテンツサーバ1001へ送信する(ステップS1325)。

10

#### 【0204】

コンテンツサーバ1001は、再生装置1004より鍵利用終了情報を受信すると、受信した鍵利用終了情報に含まれる情報IDを用いて、情報IDに対応するコンテンツ鍵情報の残数を1加算して、鍵情報テーブルT1001の更新を行う(ステップS1330)。

20

#### (5) 再生装置1003における再生時の動作

ここでは、記録媒体1002に記憶されている暗号化コンテンツを再生装置1003にて利用する場合の動作について、図31に示す流れ図を用いて説明する。

#### 【0205】

再生装置1003は、再生情報を受け付けると(ステップS1400)、受け付けた再生情報に含まれる情報IDに対応する第2鍵情報が記録媒体1002に存在するか否かの判断を行う(ステップS1405)。

ステップS1405にて第2鍵情報が存在すると判断する場合には、鍵確認処理を行う(ステップS1410)。

#### 【0206】

ステップS1405にて第2鍵情報が存在しないと判断する場合には、記録媒体を示す利用種別を含む第3要求情報を生成し、生成した第3要求情報をコンテンツサーバ1001へ送信する(ステップS1415)。

30

コンテンツサーバ1001は、第3要求情報を受信すると(ステップS1420)、記録媒体1002と互いに認証を行う(ステップS1425、ステップS1430)。

#### 【0207】

コンテンツサーバ1001は、記録媒体1002との認証が成功したか否かの判断を行う(ステップS1435)。

コンテンツサーバ1001は、ステップS1435にて認証が成功したと判断する場合には、第3要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数が「0」であるか否かを判断する(ステップS1445)。ステップS1435にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する(ステップS1485)。

40

#### 【0208】

コンテンツサーバ1001は、ステップS1445にて残数が「0」でないと判断する場合には、第2鍵情報を生成し、生成した第2鍵情報を暗号化して、再生装置1003へ送信する(ステップS1450)。ステップS1445にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する(ステップS1490)。

コンテンツサーバ1001は、第3要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数を1減算して、鍵情報テーブルT1001を更新する(ステップS1455)。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報

50

テーブルT1002に書き込む（ステップS1460）。

【0209】

記録媒体1002は、認証が成功したか否かを判断する（ステップS1440）。

記録媒体1002は、ステップS1430にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップS1480）。認証が成功したと判断する場合には、再生装置1003へ認証成功情報を出力し、再生装置1003は、コンテンツサーバ1001より暗号化された第2鍵情報を受信し、受信した暗号化された第2鍵情報を記録媒体1002へ出力する（ステップS1465）。

【0210】

記録媒体1002は、再生装置1003より暗号化された第2鍵情報を受け取り、受け取った暗号化された第2鍵情報を復号して、第2鍵情報を生成し、生成した第2鍵情報を利用鍵記憶部1102へ格納する（ステップS1470）。

再生装置1003は、記録媒体1002に格納されている第2鍵情報と暗号化コンテンツとを用いて、コンテンツを再生する（ステップS1475）。

【0211】

（6）コンテンツサーバ1001にて記録媒体1002の利用時の動作

ここでは、記録媒体1002に記憶されている暗号化コンテンツをコンテンツサーバ1001にて利用する場合の動作について、図82に示す流れ図を用いて説明する。

コンテンツサーバ1001は、格納先情報が「0」である再生情報を受け付けると（ステップS1500）、受け付けた再生情報に含まれる情報IDに対応する第2鍵情報が記録媒体1002に存在するか否かの判断を行う（ステップS1505）。

【0212】

ステップS1505にて第2鍵情報が存在すると判断する場合には、鍵確認処理を行う（ステップS1510）。

ステップS1505にて第2鍵情報が存在しないと判断する場合には、記録媒体1002と互いに認証を行う（ステップS1515、ステップS1520）。

コンテンツサーバ1001は、記録媒体1002との認証が成功したか否かの判断を行う（ステップS1525）。

【0213】

コンテンツサーバ1001は、ステップS1435にて認証が成功したと判断する場合には、受け付けた再生情報を用いて生成した第2要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数が「0」であるか否かを判断する（ステップS1535）。ステップS1525にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する（ステップS1565）。

【0214】

コンテンツサーバ1001は、ステップS1535にて残数が「0」でないと判断する場合には、第2鍵情報を生成し、生成した第2鍵情報を暗号化して、暗号化した第2鍵情報を記録媒体1002へ出力する（ステップS1540）。ステップS1535にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する（ステップS1570）。

【0215】

コンテンツサーバ1001は、第2要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数を1減算して、鍵情報テーブルT1001を更新する（ステップS1545）。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルT1002に書き込む（ステップS1550）。さらに、コンテンツサーバ1001は、記録媒体1002へ出力した第2鍵情報と、暗号化コンテンツとを記録媒体1002より読み出し、コンテンツを再生する（ステップS1555）。

【0216】

記録媒体1002は、認証が成功したか否かを判断する（ステップS1520）。

記録媒体1002は、ステップS1520にて認証が失敗したと判断する場合には、認

10

20

30

40

50

証失敗情報を利用者へ通知する（ステップS1575）。認証が成功したと判断する場合には、コンテンツサーバ1001より暗号化された第2鍵情報を受け取り、受け取った暗号化された第2鍵情報を復号して、第2鍵情報を生成し、生成した第2鍵情報を利用鍵記憶部1102へ格納する（ステップS1560）。

【0217】

（7）コンテンツサーバ1001の再生動作

ここでは、コンテンツサーバ1001に記憶されている暗号化コンテンツを再生する場合の動作について、図33に示す流れ図を用いて説明する。

コンテンツサーバ1001は、格納先情報が「1」である再生情報を受け付けると（ステップS1600）、受け付けた再生情報を用いて生成した第1要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数が「0」であるか否かを判断する（ステップS1605）。

10

【0218】

コンテンツサーバ1001は、ステップS1605にて残数が「0」でないと判断する場合には、第1鍵情報を生成し、生成した第1鍵情報を利用鍵記憶部1013へ格納する（ステップS1610）。ステップS1605にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する（ステップS1640）。

コンテンツサーバ1001は、第1要求情報に含まれる情報IDに対応するコンテンツ鍵情報の残数を1減算して、鍵情報テーブルT1001を更新する（ステップS1615）。さらに、コンテンツサーバ1001は、第1鍵情報と、暗号化コンテンツとを用いて、コンテンツを利用する（ステップS1620）。また、コンテンツ利用終了を検知すると（ステップS1625）、利用鍵記憶部1013へ格納した第1鍵情報を消去し（ステップS1630）、利用した暗号化コンテンツの情報IDに対応するコンテンツ鍵情報の残数を1加算して、鍵情報テーブルT1001の更新を行う（ステップS1635）。

20

【0219】

（8）鍵確認処理の動作

ここでは、図31にて示した鍵確認処理の動作について、図34に示す流れ図を用いて説明する。鍵確認処理は、再生装置1003の再生部1202及び利用鍵確認部1203にて行われる処理である。

利用鍵確認部1203は、存在する第2鍵情報に含まれるコンテンツ鍵が、利用期限を過ぎているか否かの判断を行う（ステップS1660）。利用期限内であると判断する場合には、再生部1202は、当該コンテンツ鍵を取得し、取得したコンテンツ鍵を用いて暗号化コンテンツを復号し、コンテンツを生成して、生成したコンテンツを再生する（ステップS1670）。

30

【0220】

利用期限でないと判断する場合には、利用鍵確認部1203は、当該コンテンツ鍵を含む第2鍵情報を削除し（ステップS1675）、利用不可情報を利用者へ通知する（ステップS1680）。

なお、図32にて示した鍵配信処理の動作についても同様であるため、説明は省略する。この場合の鍵配信処理は、コンテンツサーバ1001の再生部1017及び利用鍵確認部1019にて行われる。

40

【0221】

（9）コンテンツ鍵の事前配信時の動作

ここでは、記録媒体1002へコンテンツ鍵を事前に配信する場合の動作について、図35に示す流れ図を用いて説明する。

コンテンツサーバ1001は、事前要求情報を受け付けると、記録媒体1002へ事前要求情報を受け取った旨の情報を出力する（ステップS1700）。

【0222】

記録媒体1002は、コンテンツサーバ1001より事前要求情報を受け取った旨の情報を受け取り（ステップS1705）、コンテンツサーバ1001と互いに認証を行う（

50

ステップS1710、ステップS1715)

コンテンツサーバ1001は、記録媒体1002との認証が成功したか否かの判断を行う(ステップS1720)。

【0223】

コンテンツサーバ1001は、ステップS1720にて認証が成功したと判断する場合には、受け付けた事前配信情報に含まれる情報IDに対応するコンテンツ鍵情報の残数が「0」であるか否かを判断する(ステップS1730)。ステップS1720にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する(ステップS1755)。

【0224】

コンテンツサーバ1001は、ステップS1730にて残数が「0」でないと判断する場合には、第2鍵情報を生成し、生成した第2鍵情報を暗号化して、暗号化した第2鍵情報を記録媒体1002へ出力する(ステップS1735)。ステップS1730にて残数が「0」であると判断する場合には、残数無情報を利用者へ通知する(ステップS1760)。

【0225】

コンテンツサーバ1001は、受け付けた事前配信情報に含まれる情報IDに対応するコンテンツ鍵情報の残数を1減算して、鍵情報テーブルT1001を更新する(ステップS1740)。また、コンテンツ鍵管理情報を生成し、生成したコンテンツ鍵管理情報を配信鍵情報テーブルT1002に書き込む(ステップS1745)。

記録媒体1002は、認証が成功したか否かを判断する(ステップS1725)。

【0226】

記録媒体1002は、ステップS1725にて認証が失敗したと判断する場合には、認証失敗情報を利用者へ通知する(ステップS1765)。認証が成功したと判断する場合には、コンテンツサーバ1001より暗号化された第2鍵情報を受け取り、受け取った暗号化された第2鍵情報を復号して、第2鍵情報を生成し、生成した第2鍵情報を利用鍵記憶部1102へ格納する(ステップS1750)。

### 3. 7 鍵配信方法の変形例のまとめ

以上説明したように、鍵配信システム1000におけるコンテンツサーバ1001は、認証により鍵配信の正当性が確認され、配信要求のあったコンテンツ鍵の残数が0でない場合に、コンテンツ鍵の配信を行う。また、記録媒体1002へコンテンツ鍵を配信する場合には、コンテンツ鍵を利用することが出来る利用期間を付加することにより、記録媒体1002配信されたコンテンツ鍵の利用を制限する。これにより、常にネットワーク接続されない記録媒体1002に対してコンテンツの利用を制限することができる。

### 3. 8 変形例

上記に説明した鍵配信方法の変形例は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0227】

(1) コンテンツサーバ1001にて、コンテンツを暗号化する場合、コンテンツの情報全てを暗号化しているが、これに限定されない。コンテンツの一部のみを暗号化してもよい。

(2) 暗号化コンテンツの複製を鍵配信システム1000を構成する再生装置1004、記録媒体1002、コンテンツサーバ1001に対してのみ複製を許可するようにしてもよい。

【0228】

この場合、複製時に、複製元と複製先にて認証を行い、認証が成功した場合に複製を行うようにすればよい。

(3) または、認証が失敗する、つまり、共有秘密情報を有していない再生装置及び記録媒体に対しては、複製できる数を設定し、コンテンツサーバからのみ複製を許可するよ

10

20

30

40

50



うにしてもよい。このとき、複製が行われる度に複製できる数を1ずつ減算する。

#### 【0229】

(4) 記録媒体は、認証機能を備え、再生装置に装着されることにより利用されるIC内蔵の可搬型記録媒体であればよい。例えば、SDカードである。

または、ICを備えていない可搬型記録媒体を利用する場合には、相互認証を行わないで、コンテンツサーバ1001からの認証のみを行うようにしてもよい。

このとき、ICを備えていない可搬型記録媒体に、共通秘密情報を記憶させておき、コンテンツサーバ1001は、共通秘密情報が存在するか否かの判断による認証を行う。

#### 【0230】

ICを備えていない可搬型記録媒体は、例えば、BD (Blu-ray Disc)、DVDである。 10

または、記録媒体は、可搬型の記録媒体に限らず、携帯用の端末装置であってもよい。このとき、携帯用に端末装置は、GW1007に接続され、コンテンツサーバ1001へ利用種別が記録媒体である第3要求情報を送信し、認証が成功且つ配信可能なコンテンツ鍵の残数がある場合には、コンテンツサーバ1001から暗号化された第2鍵情報を受信することができる。携帯用の端末装置とは、例えば、PDA (Personal Digital Assistant) や、ノート型のパーソナルコンピュータである。

#### 【0231】

(5) 再生装置1003に利用鍵確認部1203を設けたが、これに限定されない。利用鍵確認部1203を記録媒体1002に備えて、再生装置1003の時計部1206、通信部1205を用いて、機能を実現してもよい。 20

また、コンテンツサーバ1001に設けた利用鍵確認部1019を、記録媒体1002に備えてもよい。

#### 【0232】

また、コンテンツサーバ1001に設けた利用鍵事前配信部1020を、記録媒体1002に備えてもよい。

(6) コンテンツサーバ1001より配信するコンテンツ鍵の総数は、どのコンテンツ鍵に対しても同一の総数であったが、これに限定されない。コンテンツ鍵ごとに異なる総数としてもよい。この場合、コンテンツ取得部1015にて、入力部1016より総数を受け付け、受け付けた総数を用いて、コンテンツ鍵情報を生成し、生成したコンテンツ鍵情報を鍵情報記憶部1031へ記憶する。 30

#### 【0233】

また、コンテンツ鍵情報の制限時間についても同様に、コンテンツ鍵ごとに異なる制限時間としてもよい。この場合、コンテンツ取得部1015にて、入力部1016より制限時間を受け付け、受け付けた制限時間を用いて、コンテンツ鍵情報を生成し、生成したコンテンツ鍵情報を鍵情報記憶部1031へ記憶する。

(7) コンテンツサーバ1001より配信するコンテンツ鍵の総数を再生装置へ配信する数と記録媒体へ配信する数とを分けて管理してもよい。

#### 【0234】

(8) 再生装置1003と再生装置1004とを同一の再生装置としてもよい。 40

(9) 記録媒体1002をコンテンツサーバ1001に装着した場合に、鍵の事前配信を可能としたが、再生装置1003に装着した場合にも、コンテンツサーバ1001からの鍵の事前配信を行えるようにしてもよい。

(10) 鍵情報テーブルT1001と配信鍵情報テーブルT1002とが分かれていたが、これらは、同一のテーブルを情報テーブルとしてもよい。

#### 【0235】

このとき、情報テーブルは、コンテンツ鍵ID、コンテンツ鍵、対応情報ID、総数、残数、制限時間及び期限情報からなる組を1個以上記憶するための領域を備える。期限情報は、利用期限〔1〕、利用期限〔2〕、・・・、利用期限〔n〕から構成される。ここで、「n」は、総数に記録されている数以上の数である。利用期限〔1〕は、上記の 50

鍵配信方法の変形例で示した利用期限と同様の情報である。また、利用期限〔2〕、  
、利用期限〔n〕については、利用期限〔1〕と同様であるため、説明は省略する。

#### 【0236】

(11) 再生装置1003において、再生装置1004と同様に、利用鍵監視部を備えてもよい。

このとき、再生装置1003の利用鍵監視部は、記録媒体1002に記憶された暗号化コンテンツの利用が終了したことを検知すると、暗号化コンテンツの利用に用いた第2鍵情報を削除し、鍵利用終了情報と、利用したコンテンツ鍵IDと、コンテンツIDに対応する利用期限とからなる情報をコンテンツサーバ1001へ送信する。

#### 【0237】

コンテンツサーバ1001は、再生装置1003より上記情報を受信すると、鍵利用終了情報に含まれる情報IDに対応するコンテンツ鍵情報の残数に1加算して、鍵情報テーブルT1001の更新を行う。また、コンテンツサーバ1001は、利用したコンテンツ鍵IDと、コンテンツIDに対応する利用期限との組に対応する情報を配信鍵情報テーブルT1002から削除する。

#### 【0238】

(12) 記録媒体1002に第2鍵情報を配信した場合、コンテンツサーバ1001にて配信した第2鍵情報に含まれるコンテンツ鍵の利用期限を管理したが、再生装置1004へ配信したコンテンツ鍵の利用期限も管理してもよい。

このとき、コンテンツサーバ1001は、再生装置1004へ第2鍵情報を送信し、再生装置1004へ配信したコンテンツ鍵IDと利用期限とからなる組を配信鍵情報テーブルT1002へ記憶する。第2鍵情報の送信後は、時間管理部1023にて、利用期限の管理を行う。

#### 【0239】

再生装置1004では、記録媒体1002に記憶された暗号化コンテンツの利用する場合と同様に、再生情報の受け付け後、受け付けた再生情報に含まれる情報IDに対応するコンテンツ鍵が存在するか否かの判断を行い、コンテンツ鍵が存在すると判断する場合には、利用期限が過ぎているか否かの判断を行う。利用期限が過ぎていると判断する場合には、当該コンテンツ鍵を含むコンテンツ鍵管理情報を消去し、利用不可情報を利用者へ通知する。利用期限内であると判断する場合には、当該コンテンツ鍵を利用して、コンテンツを生成し、再生する。

#### 【0240】

コンテンツ鍵が存在しないと判断する場合には、再生装置を示す情報が記録された利用種別と、受け取った再生情報に含まれる情報IDとを含む第3要求情報を生成し、コンテンツサーバ1001へ送信する。以降の動作は、鍵配信方法の変形例と同様であるため、説明は省略する。

また、コンテンツサーバ1001の利用鍵記憶部1013へコンテンツ鍵を出力した場合にも、上記と同様の方法で、出力したコンテンツ鍵の利用期限を管理することができる。

#### 【0241】

なお、配信される第2鍵情報は、上記の鍵配信方法の変形例と同様に暗号化されている。

(13) または、再生装置1004は、配信された第2鍵情報の管理を、コンテンツサーバ1001と同様の方法で管理してもよい。

このとき再生装置1004に時計部1310及び時間管理部1311を設ける。時計部1310は日時を計時する。時間管理部1311は、時計部1310にて計時される日時を用いて、利用鍵記憶部1302に記憶している第2鍵情報の利用期限が過ぎているか否かの判断を行う。利用期限が過ぎていると判断する場合には、当該第2鍵情報を消去し、鍵利用終了情報をコンテンツサーバ1001へ送信する。

#### 【0242】

10

20

30

40

50

また、コンテンツサーバ1001においても、時計部1026、時間管理部1023及び利用鍵記憶部1013とを用いて、上記と同様の管理が可能である。

また、記録媒体1002に時間管理部1110を設けて、上記と同様の管理を行ってもよい。この場合、上記にて示した動作は、再生装置1003に装着され、電力が供給されている間のみ行われる。

#### 【0243】

(14) または、時間管理を行う再生装置と時間管理を行わない再生装置とを区別してもよい。なお、時間管理を行う再生装置には、記録媒体も含んでいる。

このとき、時間管理を行う再生装置は、利用種別の代わりに時間管理を行う再生装置であることを示す情報を付加した第3要求情報をコンテンツサーバ1001へ送信し、時間管理を行わない再生装置は、利用種別の代わりに時間管理を行わない再生装置であることを示す情報を付加した第3要求情報をコンテンツサーバ1001へ送信する。コンテンツサーバ1001では、受信した第3要求情報を用いて、配信先の装置が、時間管理を行う再生装置であるか否かを判断し、時間管理を行う装置であると判断する場合には、暗号化された第2鍵情報を送信し、時間管理を行わない再生装置であると判断する場合には、暗号化された第1鍵情報を送信する。

#### 【0244】

(15) または、コンテンツサーバ1001のみで再生装置1004へ配信した第2鍵情報を管理してもよい。なお、第2鍵情報は、暗号化されて配信される。

このとき、再生装置1004は、装置IDを有している。ここで、装置IDとは、再生装置を識別する識別子であり、再生装置ごとに、異なる装置IDが割り当てられている。

コンテンツサーバ1001は、配信したコンテンツ鍵と利用期限と配信した再生装置1004の装置IDとを記憶している。

#### 【0245】

コンテンツサーバ1001は、第2鍵情報を再生装置1004へ送信した後、時間管理部1023にて、時計部1026で計時される日時を用いて、再生装置1004へ配信したコンテンツ鍵の利用期限が過ぎているか否かを判断し、再生装置1004へ配信したコンテンツ鍵の利用期限が過ぎたと判断する場合には、コンテンツサーバ1001から、利用期限が過ぎたコンテンツ鍵IDを含む鍵消去情報を、装置IDに対応する再生装置1004へ送信し、鍵情報テーブルにて、該当するコンテンツ鍵情報に含まれる残数を1加算する。このとき、鍵消去情報を受信した再生装置1004は、受信した情報に含まれるコンテンツ鍵IDに対応する第2鍵情報を消去する。

#### 【0246】

また、コンテンツサーバ1001の利用鍵記憶部1013へコンテンツ鍵を出力した場合にも、上記と同様の方法で、管理することができると。

また、鍵配信システム1000にて、再生装置1004と同様の構成を備える再生装置が複数ある場合には、鍵消去情報を、少なくとも1台以上の再生装置へ一括送信してもよい。この場合、鍵情報テーブルT1001にて、該当するコンテンツ鍵情報に含まれる残数に加算される数は、鍵消去情報を送信した再生装置の数である。

#### 【0247】

(16) コンテンツサーバ1001に、指定された時間に再生装置1004へ第1鍵情報を配信する機能を備えてもよい。なお、配信される第1鍵情報は、上記の鍵配信方法の変形例と同様に暗号化されている。

このとき、コンテンツサーバ1001は、さらに、コンテンツ鍵を配信する日時を示す配信日時と、配信する第1鍵情報と、配信する再生装置の装置IDとからなる自動配信情報を記憶する自動配信情報記憶部1041と、第1鍵情報を配信する日時になったか否かを管理する自動配信管理部1042と、配信する日時になった場合に、第1鍵情報を配信する指定時間配信部1043を備えている。

#### 【0248】

コンテンツサーバ1001は、再生装置1004より、コンテンツ鍵IDと、自動配信

10

20

30

40

50

を行う日時情報と、端末IDを含む自動要求情報を受け付けると、認証を行う。コンテンツサーバ1001は、認証が成功した場合に、自動配信情報を生成し、生成した自動配信情報を自動配信情報記憶部1041へ記憶し、鍵情報テーブルT1001内にて、該当するコンテンツ鍵情報に含まれる残数を1減算する。自動配信管理部1042は、時計部1026にて計時される日時を用いて、現在の日時が、自動配信情報記憶部1041に記憶している自動配信情報に含まれる配信日時になったか否かを判断し、配信日時になったと判断する場合に、指定時間配信部1043は、自動配信情報に含まれる装置IDに対応する再生装置1004へ第1鍵情報を配信し、自動配信情報記憶部1041に記憶している自動配信情報を消去する。

【0249】

なお、鍵配信システム1000にて、再生装置1004と同様の構成を備える再生装置が複数ある場合、それらの再生装置のうち少なくとも1台以上の再生装置より、同一の日時情報を受け付けた場合には、同一の日時を指定した各再生装置へ、コンテンツ鍵を一括配信してもよい。

また、自動配信情報記憶部1041に記憶する情報を、配信日時と、装置IDと、第2鍵情報とし、再生装置1004へは、上記に示した第1鍵情報の代わりに第2鍵情報を配信してもよい。

【0250】

また、記録媒体1002に対しても指定された時間に第2鍵情報を配信してもよい。この場合、自動配信情報記憶部1041に記憶する装置IDは、記録媒体1002が装着された再生装置1003の装置IDである。

また、コンテンツサーバ1001の入力部1016にて、自動要求情報を受け付けることにより、上記の動作と同様に、コンテンツサーバ1001の利用鍵記憶部1013への自動配信も可能となる。ただし、認証は行わない。

【0251】

また、コンテンツサーバ1001の入力部1016にて、コンテンツ鍵の配信先を記録媒体1002又はコンテンツサーバ1001の利用鍵記憶部1013の何れかを示す情報を付加した自動要求情報を受け付けることにより、コンテンツサーバ1001の利用鍵記憶部1013への自動配信と記録媒体1002への自動配信とを切り分けることができる。この場合、配信される情報は、第2鍵情報である。

【0252】

また、自動配信情報記憶部1041に記憶する情報を、配信日時と、装置IDとし、自動配信時に、第1鍵情報又は第2鍵情報を生成してもよい。

また、自動配信される第1鍵情報は、共通鍵暗号により暗号化して送信してもよい。自動配信される第2鍵情報も同様である。

また、自動配信時に、再度認証を行ってもよい。この認証時に生成した暗号鍵を用いて、配信される第1鍵情報又は第2鍵情報を暗号化してもよい。

【0253】

(17) 鍵配信システム1000において、配信されたコンテンツ鍵の配布先を検索する機能を追加してもよい。

このとき、再生装置1004は、コンテンツサーバ1001より指定されたコンテンツ鍵の存在を検索する鍵検索部1320を備え、また、記録媒体1002も再生装置1004と同様の鍵検索部1120を備える。

【0254】

コンテンツサーバ1001は、検索したいコンテンツ鍵に対応するコンテンツ鍵IDを含む鍵検索要求情報を同報通信的な方法により、再生装置1003及び再生装置1004へ送信する。

再生装置1004は、コンテンツサーバ1001より鍵検索要求情報を受信すると、鍵検索部1320にて、受信した鍵検索要求情報に含まれるコンテンツ鍵IDが、利用鍵記憶部1302に存在する否かの判断を行い、存在すると判断する場合には、検索要求のあ

10

20

30

40

50

ったコンテンツ鍵を所有している旨の情報をコンテンツサーバ1001へ送信する。

【0255】

再生装置1003は、コンテンツサーバ1001より鍵検索要求情報を受信すると、受信した鍵検索要求情報を記録媒体1002へ出力する。記録媒体1002は、鍵検索要求情報を受け取ると、鍵検索部1120にて、受け取った鍵検索要求情報に含まれるコンテンツ鍵IDが、利用鍵記憶部1102に存在する否かの判断を行い、存在すると判断する場合には、検索要求のあったコンテンツ鍵を所有している旨の情報をコンテンツサーバ1001へ送信する。

【0256】

また、コンテンツ鍵IDを用いて、検索を行ったが、コンテンツ鍵IDの替わりに、対応情報IDを用いてもよい。この場合も、上記と同様の方法で、検索が可能である。 10

また、記録媒体1002に鍵検索部1120を備える替わりに、再生装置1003に鍵検索部を備えてもよい。

これにより、コンテンツ鍵を配信した再生装置及び記録媒体をデータベースなどによる管理を必要とせず、検索したいコンテンツ鍵を保有する再生装置及び記録媒体を管理することができる。

【0257】

(18) コンテンツは、放送局から配信される情報としたが、これに限定されない。著作権の保護が必要な情報であればよい。

例えば、音楽情報、映像、プログラム等のデジタル化された情報である。 20

(19) 上記の鍵配信方法の変形例では、コンテンツサーバ1001から再生装置1004へ第1鍵情報を送信する際に、第1鍵情報に対応する暗号化コンテンツを送信してもよい。また、同様に、コンテンツサーバ1001から記録媒体1002へ第2鍵情報を送信する際に、第2鍵情報に対応する暗号化コンテンツを送信してもよい。

【0258】

(20) 記録媒体1002に記録される第2鍵情報は、暗号化された第2鍵情報を記憶してもよい。

例えば、コンテンツサーバ1001にて、第2鍵情報を生成後、共通秘密情報を暗号鍵として、第2鍵情報を暗号化し、暗号化した第2鍵情報(以下、「暗号化鍵情報」という。)を記録媒体1002へ配信する。記録媒体1002は、暗号化鍵情報を記憶し、利用時に共通秘密情報を用いて、暗号化鍵情報を復号して、第2鍵情報を生成して、生成した第2鍵情報を利用する。 30

【0259】

なお、暗号化鍵情報の配信時には、認証時に用いた共有秘密鍵を用いて暗号化して配信してもよい。

(21) コンテンツサーバ1001は、コンテンツサーバ1001に装着された記録媒体1002へコンテンツ鍵を出力する場合、出力する第2鍵情報を暗号化して出力したが、暗号化しないで出力してもよい。

【0260】

また、ネットワークを介して、再生装置1004へ第1鍵情報を配信する場合や記録媒体1002へ第2鍵情報を配信する場合も同様に、暗号化しないで配信してもよい。 40

(22) 配信されたコンテンツ鍵の利用回数を管理してもよい。

このとき、コンテンツ鍵を利用する度に、コンテンツ鍵の利用を示す情報をコンテンツサーバへ送信する。コンテンツサーバは、コンテンツ鍵の利用を示す情報を受け取ると、前記記録媒体へ配信したコンテンツ鍵の利用回数が、所定回数に達したか否かを判断し、所定回数に達した場合には、コンテンツ鍵に対応する残数に1加算し、記録媒体へ利用回数が所定回数に達した旨の情報を通知する。記録媒体は、利用回数が所定回数に達した旨の情報を受け取ると、コンテンツ鍵利用後、削除する。

【0261】

(23) または、コンテンツサーバにて、記録媒体へ配信したコンテンツ鍵の利用状況 50

を示す履歴情報を管理し、ある所定期間以上利用されていない場合は、前記コンテンツ鍵に対応する残数に1加算し、前記コンテンツ鍵の履歴情報に利用不可の情報を付加してもよい。

このとき、記録媒体は、配信されたコンテンツ鍵の利用を行う度に、コンテンツ鍵の利用を示す情報をコンテンツサーバへ送信する。コンテンツサーバは、コンテンツ鍵の利用を示す情報を受け取ると、記録媒体が利用するコンテンツ鍵が利用可能であるか否かを判断し、利用可能であれば、その情報を記憶する。利用可能でない場合には、利用不可を示す情報を記録媒体へ通知する。通知を受けた記録媒体は、コンテンツ鍵を削除する。

【0262】

また、コンテンツサーバでは、記憶された情報を用いて、最後にコンテンツ鍵を利用してから所定期間が過ぎたか否かを判断し、過ぎたと判断する場合に、前記コンテンツ鍵に対応する残数に1加算する。

(24) 上記の鍵配信方法の変形例にて示した利用鍵記憶部1013、利用鍵監視部1018、利用鍵確認部1019、利用鍵事前配信部1020、コンテンツ鍵制御部1021、認証部1022、時間管理部1023は、必ずしもコンテンツサーバ1001内に含まれる必要はない。例えば、コンテンツサーバ1001とは異なるネットワーク端末である鍵管理サーバを鍵配信システムの構成に追加し、鍵管理サーバ内に、利用鍵記憶部1013、利用鍵監視部1018、利用鍵確認部1019、利用鍵事前配信部1020、コンテンツ鍵制御部1021、認証部1022、時間管理部1023を備えてもよい。

【0263】

(25) 上記の鍵配信方法の変形例にて示したコンテンツ取得部1015は、放送局1006より取得する暗号化されたコンテンツを復号する復号鍵を予め記憶しているが、これに限定されない。復号鍵は、暗号化されたコンテンツとともに、放送局1006から配信されてもよい。

このとき、コンテンツ取得部1015は、放送局1006より受信部1014を介して、暗号化されたコンテンツと復号鍵とを受信することとなる。

【0264】

(26) 上記の鍵配信方法の変形例にて示したコンテンツ取得部1015は、放送局1006から取得した暗号化されたコンテンツを復号して、再度、コンテンツ鍵にて暗号化しているが、これに限定されない。暗号化されたコンテンツとその復号鍵とを、コンテンツ鍵にて暗号化して、暗号化コンテンツ情報を生成して、生成した暗号化コンテンツ情報を記憶してもよい。

【0265】

このとき、再生装置1004及び記録媒体1002へコンテンツを複製する場合には、情報IDと、暗号化コンテンツ情報が複製される。再生装置1004にて、コンテンツを利用する場合には、コンテンツサーバ1001よりコンテンツ鍵を受け取ると、受け取ったコンテンツ鍵を用いて、暗号化コンテンツ情報を復号して、暗号化されたコンテンツと、その復号鍵とを生成して、生成した復号鍵を用いて、暗号化されたコンテンツを復号する。また、再生装置1003にて、記録媒体1002に記録されているコンテンツを利用する場合も同様の動作にて、暗号化されたコンテンツを復号する。

【0266】

(27) 上記鍵配信方法の変形例及び上記変形例をそれぞれ組み合わせるとしてもよい。

#### 4. AD内サーバに係る変形例

前記AD内サーバ100は、コンテンツの複製に関し、グループ内装置に対して複製を許可するための管理情報と、グループ外の装置に対して複製を許可するための管理情報とを管理してもよい。

【0267】

以下に、前記AD内サーバが、前記グループ内及びグループ外装置それぞれに対する管理情報を保持する場合について説明する。

10

20

30

40

50

コンテンツの再生装置と、ホームサーバとの間のグループ登録手順、脱退手順については、前記した手順で行うものとし説明は省略する。

以下の説明では、グループ形成管理システムをコンテンツ複製管理システムと称し、前記A D内サーバをホームサーバと称する。

#### 4. 1 概要

図36は、コンテンツ複製管理システム2000の構成を示すブロック図である。

##### 【0268】

ホームサーバ2001と、再生装置2002と、再生装置2003とは、ゲートウェイ2005を介して接続し、家庭内ネットワークを形成する。

記憶媒体2004は、再生装置2003が備える挿入口に挿入されることにより、再生装置2003と接続する。 10

家庭内ネットワークにおいて、ホームサーバ2001と、再生装置2002と、再生装置2003とは、それぞれTCP/IPを用いて通信を行う。

##### 【0269】

ゲートウェイ2005が前記家庭内ネットワークと、外部ネットワークとの間のルーティング処理を行う。

再生装置2006と、放送局2007とは、前記外部ネットワークに接続する。

放送局2007は、地上波デジタル放送を行う放送局であり、UHF帯の電波を用いて、番組を各家庭に向けて放送する。

##### 【0270】

20

ホームサーバ2001は、地上波デジタル放送受信機能を備え、放送局2007の放送内容を受信し、前記放送内容を所定の形式のデジタルデータに加工し、コンテンツとして大容量ハードディスクに蓄積する。

ホームサーバ2001は、再生装置2002、再生装置2003、再生装置2006に対する前記コンテンツの複製管理を行う。

##### 【0271】

再生装置2002、再生装置2003、再生装置2006は、ホームサーバ2001から前記コンテンツの複製許可を受けた場合に、前記コンテンツをホームサーバ2001から取得して記憶し、再生を行う。

本変形例では、家庭内ネットワークの範囲内をグループ2010とする。

30

グループ内においては、前記コンテンツの複製に関する制限が緩和される。

##### 【0272】

グループ2010には、ホームサーバ2001、再生装置2002、再生装置2003、ゲートウェイ2005、記憶媒体2004が属している。

前記外部ネットワークに属する装置は、家庭内ネットワーク或いはグループ2010の管理者が、管理出来ない装置である。

ホームサーバ2001は、外部ネットワークに属する装置へ前記コンテンツを複製する場合、グループ2010内の装置への複製よりも、厳しい制限を行う必要がある。

##### 【0273】

ホームサーバ2001は、前記コンテンツの複製を許可する数により、前記制限を行う 40

ホームサーバ2001は、前記コンテンツの複製を許可する上限数を、グループ2010内と、家庭内ネットワークの範囲外であるグループ外とで分けて管理する。

グループ2010に属する装置や記憶媒体は、グループ2010に属していることを示す共通の情報であるグループ所属情報を、それぞれ保持する。

##### 【0274】

前記グループ所属情報は、秘密的に各装置、記憶媒体に配布された共通秘密情報、第三者である認証機関が発行したグループを構成する機器の機器リストから成る。

#### 4. 2 構成

##### 4. 2. 1 ホームサーバ2001

50

ホームサーバ 2001 は、具体的には、ネットワーク通信機能と、大容量記憶領域を持つハードディスクとを備える DVD プレーヤー等である。

【0275】

図 37 は、ホームサーバ 2001 の構成を示すブロック図である。

通信部 2101 は、ネットワークを介して、他の装置と TCP/IP による通信を行う。

複製制限情報管理部 2102 は、コンテンツの複製に係る制御を行う。

図 38 は、複製制限情報管理部 2102 が保持する情報を示す。

【0276】

図 38 (a) は、複製制限情報管理部 2102 が保持する複製制限情報を示す。

10

前記複製制限情報は、コンテンツに対応づけられた情報であり、コンテンツ識別子と、グループ内装置残数と、グループ外装置残数と、グループ内媒体残数と、グループ外媒体残数と、使用期限情報とから成る。

前記複製制限情報は、放送局 2007 から放送により取得するコンテンツに関する情報であり、放送局 2007 から送信される放送とは別に、ネットワークを通じて放送局 2007 から取得する。

【0277】

前記コンテンツ識別子は、各コンテンツに割り当てられたコンテンツを一意に識別する識別子である。

グループ内装置残数は、前記グループ内の装置に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

20

前記グループ内の装置に、前記コンテンツを複製した場合、複製制限情報管理部 2102 は、前記グループ内装置残数を 1 減少させる。

【0278】

前記グループ内の装置が、複製した前記コンテンツを消去した場合、複製制限情報管理部 2102 は、前記グループ内装置残数を 1 増加させる。

グループ外装置残数は、グループ外の装置に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

前記グループ外の装置に、前記コンテンツを複製した場合、複製制限情報管理部 2102 は、前記グループ外装置残数を 1 減少させる。

30

【0279】

前記グループ外の装置が、複製した前記コンテンツを消去した場合であっても、複製制限情報管理部 2102 は、前記グループ内装置残数を 1 増加させない。

前記グループ内媒体残数は、グループ内の記憶媒体に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

前記グループ外媒体残数は、グループ外の記憶媒体に、前記コンテンツ識別子で示されるコンテンツを、複製できる残りの数を示す。

【0280】

例えば、グループ 2010 内の再生装置 2002 がサーバ 2001 に対しコンテンツの複製を要求する場合、複製制限情報管理部 2102 は、グループ内装置残数が 1 以上である場合、前記要求に対し許可を与え、グループ内装置残数が 0 である場合は、前記要求に対し却下を通知する。

40

ホームサーバ 2001 から再生装置 2002 にコンテンツを複製する場合、複製制限情報管理部 2102 は、グループ内装置残数を 1 減少させる。

【0281】

また、再生装置 2002 が、複製したコンテンツの消去をサーバ 2001 に通知した場合、複製制限情報管理部 2102 は、グループ内装置複製残数を 1 増加させる。

前記使用期限情報は、前記コンテンツの使用可能な期限を示す情報である。

例えば、前記使用期限情報は、2005 年 6 月 30 日といった具体的な日時を示す。

複製制限情報管理部 2102 は、前記使用期限情報が定められてコンテンツを複製した

50



場合、前記使用期限情報を時刻管理部2105が備えるタイマーに通知し、前記使用期限情報が示す時刻に、使用期限到達通知を出力するよう指示する。

【0282】

複製制限情報管理部2102は、時刻管理部2105から前記使用期限到達通知を取得した場合に、前記複製したコンテンツの使用が終了すると判定し、グループ内装置複製残数を1増加させる。

使用期限管理処理については、後述する。

複製制限情報管理部2102は、コンテンツの複製を要求する要求装置から、前記要求装置が複製を希望するコンテンツを識別するコンテンツ確認情報を含むコンテンツ確認要求を、ブロードキャストにより受信する。

10

【0283】

前記ブロードキャストを受信した場合、複製制限情報管理部2102は、通信部2101を介して、前記コンテンツ確認情報と一致するコンテンツ識別子を含む複製制限情報を管理しているか否かを確認し、保持している場合、ブロードキャストの送信元装置に対し、複製可を示す複製可否通知を送信する。

また、ICMP (Internet Control Message Protocol) エコームッセージを受信した場合、複製制限情報管理部2102は、ICMPエコーリプライメッセージを送信元装置に対し送信する。

【0284】

複製制限情報管理部2102は、コンテンツ複製を要求する要求装置から、複製を希望するコンテンツを識別する前記コンテンツ確認情報と、記憶媒体が装置かの区分を示す装置属性情報を含むコンテンツ複製要求を受信し、認証部2103に対し認証開始指示を送信する。

20

複製制限情報管理部2102は、前記コンテンツ複製要求に基づき要求管理情報を生成する。

【0285】

前記要求管理情報は、複製が消去かの区別を示す処理区分と、コンテンツを識別する前記コンテンツ確認情報と、前記要求装置のIPアドレスと、前記要求装置がグループ内かグループ外かを示す前記グループ内外情報と、要求装置が媒体か装置のいずれかを示す装置属性情報と、予約情報と、次の要求管理情報を保持している場所を示す次要求ポイントとから成る。

30

【0286】

前記予約情報は、前記コンテンツの複製或いは消去を開始する時刻を示す。

例えば、前記予約情報は、2005年6月30日といった具体的な日時を示す。

複製制限情報管理部2102は、コンテンツの複製を要求する要求装置から、前記予約情報をコンテンツの複製予約要求と共に取得する。

図38(b)は、前記要求管理情報をキューを用いて管理する要求管理キューを示す図である。

【0287】

図38(b)では、前記要求管理キューに、前記要求管理情報が3つ繋がっている例を示している。

40

複製制限情報管理部2102は、前記コンテンツ複製要求を受信した場合、前記コンテンツ複製要求に含まれるコンテンツ確認情報と、前記装置属性情報と、要求装置のIPアドレスとを生成した前記要求管理情報に書き込む。

【0288】

複製制限情報管理部2102は、認証部2103から前記グループ内外情報を取得して、前記要求管理情報に書き込む。

ホームサーバ2001は、要求先頭ポイントが指す要求管理情報が示す要求から順に、対応する処理を行う。

前記対応する処理が終わると、複製制限情報管理部2102は、前記要求先頭ポイント

50

の内容を、前記要求管理情報内の次要求ポイントが示す要求管理情報を指すように書き換える。

【0289】

また、新たな要求を他装置から取得した場合、複製制限情報管理部2102は、取得した要求に応じた要求管理情報を新たに作成し、キューの最後に繋ぐ。

前記要求管理情報中の前記処理区分が、複製を示す場合、前記要求管理情報中の前記グループ内外情報と、前記装置属性情報との組み合わせに基づき、処理の対象となる対象残数をグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ内媒体残数から1つ選択する。

【0290】

例えば、前記グループ内外情報がグループ内を示し、前記装置属性情報が装置を示す場合、前記対象残数は、グループ内装置残数となり、前記グループ内外情報がグループ内を示し、前記装置属性情報が媒体を示す場合、前記対象残数は、グループ内媒体残数となる

次に、前記要求管理情報中のコンテンツ確認情報に一致するコンテンツ識別子を持つ複製制限管理情報中の、前記対象残数が0か否かを調べる。

【0291】

複製制限情報管理部2102は、前記対象残数が0でない場合、前記コンテンツ識別子で識別されるコンテンツが、複製可であると判定し、0であった場合は、複製不可と判定する。

複製可であった場合、前記コンテンツを暗号化し、前記要求装置に送信するよう、暗号復号化部2104に指示する。

【0292】

暗号復号化部2104は、前記指示に従い前記コンテンツを暗号化し、前記要求装置に送信する。

前記要求管理情報中の前記処理区分が、消去を示す場合、複製制限情報管理部2102は、前記要求管理情報中の前記グループ内外情報と、前記装置属性情報との組み合わせに基づき、処理の対象となる対象残数をグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ内媒体残数から1つ選択する。

【0293】

複製制限情報管理部2102は、前記要求装置に対し、返却処理開始通知を送信する。

また、複製制限情報管理部2102は、前記要求装置から、コンテンツ消去完了通知を受信した場合、前記要求管理情報中のコンテンツ確認情報に一致するコンテンツ識別子を持つ複製制限管理情報中の、前記対象残数を1増加させる。

複製制限情報管理部2102は、キュー先頭の前記要求管理情報を削除し、前記要求管理キューを更新する。

【0294】

また、複製制限情報管理部2102は、要求装置から、複製制限管理情報の譲渡要求を受信する。

複製制限情報管理部2102は、管理している前記複製制限管理情報の一部或いは全てを他の装置に譲渡する処理を行う。

複製制限管理情報譲渡処理については、後述する。

【0295】

複製制限情報管理部2102は、コンテンツの複製を要求する要求装置から、通信部2101を介して、複製予約要求を受信する。

前記複製予約要求は、複製要求に係るコンテンツを示すコンテンツ情報と、コンテンツの複製を開始する時刻を示す前記予約情報とを含む。

複製制限情報管理部2102は、前記複製予約要求を受信した場合、前記複製予約要求に含まれる前記コンテンツ指定情報に一致する前記コンテンツ識別子を保持しているか判定し、保持している場合は、前記複製開始時刻情報を前記コンテンツ識別子に対応づけて

10

20

30

40

50

保持する。

【0296】

また、時刻管理部2105が備えるタイマーに対し、前記複製開始時刻情報を通知し、前記複製開始時刻情報が示す時刻に、予約時刻到達通知を出力するよう指示する。

複製制限情報管理部2102は、前記予約時刻到達通知を取得した場合、前記コンテンツの複製を実行する。

予約管理処理については、後述する。

【0297】

認証部2103は、複製制限情報管理部2102から、前記認証開始指示を受信し、コンテンツの複製を要求する要求装置との間で、相互認証と鍵共有を実行する。

10

また、認証部2103は、グループ2010に属していることを示す情報であるグループ所属情報を保持する。

前記グループ所属情報は、秘匿的に各装置、記憶媒体に配布された共通秘密情報、第三者である認証機関が発行したグループを構成する機器の機器リストから成る。

【0298】

前記相互認証と鍵共有については、後述する。

前記相互認証と鍵共有が成功した場合には、認証部2103と、前記要求装置とは、同一の鍵であるセッション鍵を共有する。

認証部2103は、前記セッション鍵を保持し、かつ、暗号復号化部2104に前記セッション鍵を通知する。

20

【0299】

また認証部2103は、要求装置から、グループ所属情報を受信する。

前記受信したグループ所属情報と、保持しているグループ所属情報とが一致するか否かを判定し、一致する場合グループ内を示す、一致しない場合グループ外を示すグループ内外情報を、複製制限情報管理部2102に通知する。

暗号復号化部2104は、認証部2103が行う前記相互認証と鍵共有が成功した後、認証部2103から前記セッション鍵を取得する。

【0300】

暗号復号化部2104は、前記相互認証と鍵共有が成功した後に、前記要求装置へ送信するデータの暗号化、前記要求装置から受信したデータの復号化を、前記セッション鍵を用いて行う。

30

時間管理部2105は、時計と、タイマーを備える。

前記時計は、例えば、1秒毎にカウントアップし、1970年1月1日0時0分0秒からの秒数を示すカウンタで構成する。

【0301】

前記タイマーには、通知要求元から、タイマー通知要求時刻が設定される。

前記タイマーは、前記時計が、前記タイマー通知要求時刻で示される時刻を指したとき、前記通知要求元に対し、設定した時刻に到達したことを示す通知を行う。

地上波デジタル放送受信部2106は、放送局2007から番組を受信する。

地上波デジタル放送受信部2106は、受信した放送波に対し、規定の方法により復調、多重分離、復号等を行うことにより、映像情報、音声情報、データ放送用情報、コンテンツ識別子を含むその他コンテンツ再生に必要な制御情報等を取得する。

40

【0302】

地上波デジタル放送受信部2106は、前記映像情報、音声情報及びデータ放送用情報を、パーシャルTS等の所定の形式のデジタルデータに変換し、記憶部2107にコンテンツとして出力する。

記憶部2107は、地上波デジタル放送受信部2106から受信した前記コンテンツを、前記コンテンツ識別子と対応づけて蓄積する。

【0303】

記憶部2107は、耐タンパ機能を有し、保持する情報を、装置外部から知られること

50

はない。

#### 4. 2. 2 再生装置 2002

再生装置 2002 は、具体的には、ネットワーク通信機能と、大容量記憶領域を持つハードディスクとを備える DVD プレーヤー等である。

##### 【0304】

図 39 は、再生装置 2002 の構成を示すブロック図である。

通信部 2201 は、ネットワークを介して、他の装置と TCP/IP による通信を行う

複製制限情報管理部 2202 は、コンテンツの複製管理を行う。

複製制限情報管理部 2202 の動作は、複製制限情報管理部 2102 とほぼ同じである  
ので、異なる動作について説明する。 10

##### 【0305】

複製制限情報管理部 2202 は、コンテンツの複製元装置に対し、複製を希望するコンテンツを識別する前記コンテンツ確認情報と、記憶媒体が装置かの区分を示す装置属性情報を含むコンテンツ複製要求を送信する。

前記装置属性情報は、コンテンツの複製要求を行う主体が、再生装置 2002 のような装置の場合は装置を示し、IC 内蔵可搬型記憶媒体 2004 のように記憶媒体の場合は媒体を示す情報である。

##### 【0306】

よって、再生装置 2002 が送信する前記装置属性情報は、装置を示す。 20

複製制限情報は、コンテンツの配布を行うサーバが管理する。

再生装置 2002 は、コンテンツの複製を許可する権限を持つホームサーバ 2001 から、前記複製を許可する権限の譲渡を受けることにより、コンテンツを配布する権限を持つこととなる。

##### 【0307】

複製制限情報管理部 2202 は、ホームサーバ 2001 から、前記コンテンツ識別子と、前記グループ内装置残数と、前記グループ外装置残数と、前記グループ内媒体残数と、前記グループ外媒体残数と、前記使用期限情報とを取得し、前記複製制限情報として保持する。

前記複製を許可する権限の譲渡を受けた複製制限情報管理部 2202 は、複製制限情報  
管理部 2102 と同じ構成である。 30

##### 【0308】

ここで、再生装置 2002 は、取得した前記コンテンツ識別子に対応するコンテンツを保持する必要はなく、他の装置が、前記コンテンツ識別子に対応するコンテンツを保持していてもよい。

この場合、他の装置から前記コンテンツの複製の要求を受け、前記コンテンツの複製を許可する場合、前記コンテンツを保持している装置に対し、前記コンテンツを、前記複製要求を行った装置に対し送信するよう指示する。

##### 【0309】

また、ホームサーバ 2001 から取得する前記グループ内装置残数と、前記グループ外  
装置残数と、前記グループ内媒体残数と、前記グループ外媒体残数とは、前記ホームサ  
ーバ 2001 が保持する残数の全てではなく一部でもよい。 40

例えば、ホームサーバ 2001 は、前記グループ内装置残数として値「10」を保持している場合に、再生装置 2002 に対し、前記グループ内装置残数として値「5」だけ譲渡してもよい。

##### 【0310】

上記の場合、再生装置 2002 は、グループ内の装置に対し、前記コンテンツを 5 つまで、複製許可する権限を持つ。

また、再生装置 2002 は、ホームサーバ 2001 から取得した前記複製制限情報の一部或いは全てを返却してもよい。 50

再生装置 2002 は、ホームサーバ 2001 に対し、前記グループ内装置残数として値「2」だけ返却してもよい。

#### 【0311】

前記複製制限情報の譲渡と返却については後述する。

認証部 2203 は、認証相手である認証装置と、相互認証と鍵共有を実行する。

認証部 2203 は、グループ 2010 に属していることを示す情報である前記グループ所属情報を保持する。

前記相互認証と鍵共有については、後述する。

#### 【0312】

前記相互認証と鍵共有が成功した場合には、認証部 2203 と、前記認証装置とは、同一の鍵であるセッション鍵を共有する。 10

認証部 2203 は、前記セッション鍵を保持し、かつ、暗号復号化部 2204 に前記セッション鍵を通知する。

暗号復号化部 2204 は、認証部 2203 が行う前記相互認証と鍵共有が成功した後、認証部 2203 から前記セッション鍵を取得する。

#### 【0313】

暗号復号化部 2204 は、前記相互認証と鍵共有が成功した後に、前記認証装置へ送信するデータの暗号化、前記認証装置から受信したデータの復号化を、前記セッション鍵を用いて行う。

時間管理部 2205 は、時計と、タイマーを備える。 20

前記時計は、例えば、1秒毎にカウントアップし、1970年1月1日0時0分からの秒数を示すカウンタで構成する。

#### 【0314】

前記タイマーには、通知要求元から、タイマー通知要求時刻が設定される。

前記タイマーは、前記時計が、前記タイマー通知要求時刻で示される時刻を指したとき、前記通知要求元に対し、設定した時刻に到達したことを示す通知を行う。

コンテンツ配布元決定部 2206 は、サーバ或いはコンテンツの複製権を譲渡された装置の中から、コンテンツの複製許可を受ける装置である配布元装置を決定する。

#### 【0315】

コンテンツ配布元決定部 2206 は、ネットワーク上に、複製を希望するコンテンツを示すコンテンツ識別情報を含むコンテンツ確認情報をブロードキャストをする。 30

コンテンツ配布元決定部 2206 は、前記コンテンツ確認情報に回答してきた装置に対し、順番に、ICMP (Internet Control Message Protocol) エコーメッセージを送信し、前記送信時から、応答である ICMP エコーリプライメッセージを受信するまでの応答時間を測定していく。

#### 【0316】

コンテンツ配布元決定部 2206 は、応答時間が最短であった装置を配布元装置に決定し、前記配布元装置を、複製制限情報管理部 2202 に通知する。

記憶部 2207 は、コンテンツの保持を行う。

再生部 2208 は、記憶部 2207 に保持しているコンテンツ、或いは通信部 2201 が受信したコンテンツの再生を行う。 40

#### 4. 2. 3 再生装置 2003

再生装置 2003 は、具体的には、ネットワーク通信機能を備えた SD プレーヤーである。

#### 【0317】

図 40 は、再生装置 2003 と IC 内蔵可搬型記憶媒体 2004 との構成を示すブロック図である。

通信部 2301 は、ネットワークを介して、他の装置と TCP/IP による通信を行う

通信部 2303 は、IC 内蔵可搬型記憶媒体と接続し、通信を行う。

## 【0318】

再生部2302は、IC内蔵可搬型記憶媒体から読み出すコンテンツを再生する。

## 4. 2. 4 IC内蔵可搬型記憶媒体2004

IC内蔵可搬型記憶媒体2004は、具体的には、ICを内蔵する、耐タンパ性を有したSDカードである。

入出力部2311は、再生装置2003との通信を行う。

## 【0319】

IC内蔵可搬型記憶媒体2004は、再生装置2003を介して、他の装置と通信を行う。

コンテンツ配布元決定部2312の説明は、前述したコンテンツ配布元決定部2206と同じ説明となる。 10

コンテンツ配布元決定部2312は、決定した配布元装置に対し、コンテンツ識別情報を含むコンテンツ複製要求を送信する。

## 【0320】

認証部2313は、認証を行う相手である認証装置と、再生装置2003及びネットワークを介して通信を行い、相互認証と鍵共有を実行する。

認証部2313は、グループ2010に属していることを示す情報である前記グループ所属情報を保持する。

相互認証と鍵共有については後述する。

## 【0321】

前記相互認証と鍵共有が成功した場合には、認証部2313と、前記認証装置とは、同一の鍵であるセッション鍵を共有する。 20

認証部2313は、前記セッション鍵を保持し、かつ、暗号復号化部2314に前記セッション鍵を通知する。

暗号復号化部2314は、認証部2313が行う前記相互認証と鍵共有が成功した後、認証部2313から前記セッション鍵を取得する。

## 【0322】

暗号復号化部2314は、前記相互認証と鍵共有が成功した後に、前記認証装置へ送信するデータの暗号化、前記認証装置から受信したデータの復号化を、前記セッション鍵を用いて行う。 30

記憶部2315は、コンテンツの保持を行う。

## 4. 2. 5 再生装置2006

再生装置2006は、具体的には、ネットワーク通信機能、大容量のハードディスクを備えたDVDプレーヤー等である。

## 【0323】

図41は、再生装置2006の構成を示すブロック図である。

通信部2401は、ネットワークを介して、他の装置とTCP/IPによる通信を行う。

認証部2402は、コンテンツを保持するサーバとの間で、相互認証と鍵共有を実行する。 40

## 【0324】

但し、認証部2402は、前記グループ所属情報を保持しないため、ホームサーバ2001において、再生装置2006がグループ外の装置であると判定される。

前記相互認証と鍵共有については、後述する。

前記相互認証と鍵共有が成功した場合には、認証部2402と、前記サーバとは、同一の鍵であるセッション鍵を共有する。

## 【0325】

認証部2402は、前記セッション鍵を保持し、かつ、暗号復号化部2403に前記セッション鍵を通知する。

暗号復号化部2403は、認証部2402が行う前記相互認証と鍵共有が成功した後、 50

認証部 2402 から前記セッション鍵を取得する。

暗号復号化部 2403 は、前記相互認証と鍵共有が成功した後に、前記認証装置へ送信するデータの暗号化、前記認証装置から受信したデータの復号化を、前記セッション鍵を用いて行う。

【0326】

記憶部 2404 は、コンテンツの保持を行う。

#### 4. 3 動作

##### 4. 3. 1 コンテンツ複製元決定処理

コンテンツの複製を要求する要求装置は、ネットワーク上の装置の中から、所望のコンテンツの複製元となる配信装置を決定する。

10

【0327】

図 42 は、コンテンツ複製元決定処理を示すフローチャートである。

ここでは、要求装置は再生装置 2002 であり、配信装置はホームサーバ 2001 であり、他装置は再生装置 2003 であるものとする。

前記配信装置は、コンテンツ複製元決定処理において結果的に、前記配信装置からコンテンツ複製元として選択された装置を示す。

【0328】

前記他装置は、コンテンツ複製元決定処理において、結果的に、前記配信装置からコンテンツ複製元として選択されなかった装置を示す。

前記要求装置は、コンテンツを要求する装置であり、再生装置 2003 が、コンテンツの複製要求を行う場合であれば、再生装置 2003 が前記要求装置となる。

20

前記要求装置は、所望のコンテンツ識別情報が示すコンテンツを、いずれの装置から複製してもらおうかを決定する。

【0329】

前記要求装置は、所望のコンテンツを保持している装置から応答を取得する目的で、コンテンツ確認要求をネットワーク上にブロードキャスト送信する (S2001)。

前記コンテンツ確認要求は、要求装置が複製を希望するコンテンツを識別するコンテンツ確認情報を含む。

前記配信装置及び前記他装置は、前記コンテンツ確認要求を受信する。

【0330】

30

前記配信装置は、前記コンテンツ確認要求中の前記コンテンツ確認情報と一致するコンテンツ識別子を管理しているか確認する (S2002)。

前記他装置は、前記コンテンツ確認情報と一致するコンテンツ識別子を保持しているか確認する (S2003)。

前記配信装置は、一致するコンテンツ識別子を管理している場合 (S2002: YES)、複製可を示す複製可否通知を要求装置へ送信する (S2004)。

【0331】

前記配信装置は、一致するコンテンツ識別子を管理していない場合 (S2002: NO)、処理を終了する。

前記他装置は、一致するコンテンツ識別子を管理している場合 (S2003: YES)、複製可を示す複製可否通知を要求装置へ送信する (S2005)。

40

前記他装置は、一致するコンテンツ識別子を管理していない場合 (S2003: NO)、処理を終了する。

【0332】

前記要求装置は、受信した各複製可否通知の内容を確認し、複製可を示す複製可否通知を送信した装置の送信元 IP アドレスを保持する (S2006)。

前記要求装置は、前記保持した IP アドレスを持つ各装置に対し、ICMP (Internet Control Message Protocol) エコーメッセージを送信し、前記送信時から、応答である ICMP エコーリプライメッセージを受信するまでの応答時間を測定する。

50

## 【0333】

前記要求装置は、前記配信装置に対し、ICMPエコーメッセージを送信する(S2007)。

前記配信装置は、ICMPエコーメッセージを受信し、応答として前記要求装置に対し、ICMPリプライメッセージを送信する(S2008)。

前記要求装置は、ICMPエコーリプライメッセージを受信し、測定した前記応答時間を保持する。

## 【0334】

前記要求装置は、前記他装置に対し、ICMPエコーメッセージを送信する(S2009)。

前記他装置は、ICMPエコーメッセージを受信し、応答として前記要求装置に対し、ICMPエコーリプライメッセージを送信する(S2010)。

前記要求装置は、ICMPエコーリプライメッセージを受信し、測定した前記応答時間を保持する。

## 【0335】

前記要求装置は、複製元装置として、前記応答時間が最短であった装置を選択し、複製元装置のIPアドレスを保持しておく(S2011)。

## 4. 3. 2 相互認証と鍵共有

図43及び図44は、配信装置と要求装置との間で行われる相互の機器認証及び鍵共有の動作を示すフローチャートである。

## 【0336】

ここでは、再生装置2002が、図42に示したコンテンツ複製元決定処理により、複製元としてホームサーバ2001を選択したものとする。

よって、配信装置はホームサーバ2001であり、要求装置は再生装置2002である例で説明する。

ホームサーバ2001の認証部2103は、著作権保護ライセンサ(CA)の公開鍵PK-CA、秘密鍵SK-A及び公開鍵証明書Cert-CAを予め記憶しており、楕円曲線Eによる暗号処理部を有している。

## 【0337】

また、再生装置2002の認証部2203は、著作権保護ライセンサの公開鍵PK-CA、秘密鍵SK-i及び公開鍵証明書Cert-iを予め記憶しており、楕円曲線Eによる暗号処理部を有している。

また、S19(SK、D)は、秘密鍵SKを用いてデータDにデジタル署名を施す演算である。

## 【0338】

また、Gは、楕円曲線E上のベースポイントであり、本認証システムに固有の値である。

また、「\*」は、楕円曲線E上の乗算を示す演算子である。

例えば、「 $\times * G$ 」は、楕円曲線E上の点Gを $\times$ 個、加算する演算である。

「||」は、結合を示す演算子であり、例えば、「A||B」は、「A」と「B」との結合結果である。

## 【0339】

以下において、「認証部2103は、認証部2203へ情報を出力する」及び「認証部2203は、認証部2103へ情報を出力する」などは、簡略化した記載であり、それぞれ、「認証部2103は、通信部2101及び通信部2201を介して、認証部2203へ情報を出力する」及び「認証部2203は、通信部2201及び通信部2101を介して、認証部2103へ情報を出力する」を意味するものである。

## 【0340】

認証部2203は、乱数 $\gamma$ を生成し(S2101)、生成した乱数 $\gamma$ 及び公開鍵証明書Cert-iを認証部2103へ出力する(S2102)。

10

20

30

40

50



認証部 2103 は、乱数  $\gamma$  及び公開鍵証明書  $Cert_{\gamma}$  を受け取り (S2102)、CRL (Certificate Revocation List) を用いて、再生装置 2002 の公開鍵証明書  $Cert_{\gamma}$  が無効化されていないかどうかを確認する (S2103)。

#### 【0341】

無効化されている場合 (S2104: NO)、処理を終了する。

無効化されていない場合 (S2104: YES)、認証部 2103 は、公開鍵  $PK-C$  A を用いて公開鍵証明書  $Cert_{\gamma}$  の検証を行う (S2105)。

検証に失敗すると (S2106: NO)、認証部 2103 は、処理を終了する。

検証に成功すると (S2106: YES)、認証部 2103 は、乱数  $x$  を生成し (S2107)、生成した乱数  $x$  及び公開鍵証明書  $Cert_{\gamma}$  A を認証部 2203 へ出力する (S2108)。

#### 【0342】

認証部 2203 は、認証部 2103 から乱数  $x$  及び公開鍵証明書  $Cert_{\gamma}$  A を受け取る (S2108)。

次に、認証部 2203 は、CRL を用いて、ホームサーバ 2001 の公開鍵証明書  $Cert_{\gamma}$  A が無効化されていないかどうかを確認する (S2109)。

無効化されている場合 (S2110: NO)、認証部 2203 は、処理を終了する。

#### 【0343】

無効化されていない場合 (S2110: YES)、認証部 2203 は、公開鍵  $PK-C$  A を用いて公開鍵証明書  $Cert_{\gamma}$  A の検証を行う (S2111)。

検証に失敗すると (S2112: NO)、認証部 2203 は、処理を終了する。

検証に成功すると (S2112: YES)、認証部 2203 は、乱数  $\gamma'$  を生成し (S2113)、署名データ  $S1 = \text{Sig}(SK_{\gamma'}, (\gamma' * G) || x)$  を生成し (S2114)、 $\gamma' * G$  及び  $S1$  を認証部 2103 へ出力する (S2115)。

#### 【0344】

認証部 2103 は、認証部 2203 から  $\gamma' * G$  及び  $S1$  を受け取る (S2115)。

次に、認証部 2103 は、 $S1$  の検証を行う (S2116)。

検証に失敗した場合は (S2117)、認証部 2103 は、処理を終了する。

検証に成功した場合 (S2117)、認証部 2103 は、乱数  $x'$  を生成し (S2118)、署名データ  $S0 = \text{Sig}(SK_A, (x' * G) || \gamma)$  を生成し (S2119)、 $x' * G$  及び  $S0$  を認証部 2203 へ出力する (S2120)。

#### 【0345】

認証部 2203 は、認証部 2103 から  $x' * G$  及び  $S0$  を受け取り (S2120)、次に、認証部 2203 は、 $S0$  の検証を行う (S2121)。

検証に失敗すると (S2122: NO)、認証部 2203 は、処理を終了する。

検証に成功すると (S2122: YES)、認証部 2203 は、セッション鍵  $K' = \gamma' (x' * G)$  を算出する (S2124)。

#### 【0346】

一方、認証部 2103 は、認証部 2203 は、セッション鍵  $K = x' (\gamma' * G)$  を算出する (S2123)。

以上のようにして、ホームサーバ 2001 及び再生装置 2002 の間の相互の機器認証と鍵共有が行われる。

セッション鍵  $K$  及び  $K'$  は、それぞれホームサーバ 2001 及び再生装置 2002 において共有される同一の値を有する鍵である。

### 4. 3. 3 コンテンツ複製処理

図 45 は、コンテンツの複製処理を示す図である。

#### 【0347】

図 45 中、要求装置が再生装置 2002 であり、配信装置がホームサーバ 2001 であり、他装置が再生装置 2003 である場合を例として説明する。

前記配信装置と、前記要求装置と、前記他装置とは、図42に示すコンテンツ複製元決定処理を行う(S2201)。

前記要求装置は、前記コンテンツ複製元決定処理により、複製元である配信装置としてホームサーバ2001を選択したものとする。

#### 【0348】

前記要求装置は、前記配信装置に対し、複製を希望するコンテンツを識別する前記コンテンツ確認情報と、記憶媒体が装置かの区分を示す前記装置属性情報を含むコンテンツ複製要求を送信する(S2202)。

前記配信装置は、前記コンテンツ複製要求を受信し、前記要求装置のIPアドレスと共に保持する。

10

#### 【0349】

前記配信装置と、前記要求装置とは、図43及び図44に示した、相互認証と鍵共有を行う(S2203)。

前記配信装置と、前記要求装置とは、S2203の実行結果としてセッション鍵を共有する。

前記配信装置と前記要求装置とは、セッション鍵の共有が完了した以降の通信を、前記セッション鍵を用いて暗号化及び復号化する。

#### 【0350】

前記要求装置は、前記グループ所属情報を、前記配信装置に送信する(S2204)。

前記要求装置は、受信した前記グループ所属情報と、認証部2103で保持しているグループ所属情報とが一致しているか否かを判定する(S2205)。

20

前記配信装置は、S2203において、相互認証と鍵共有が成功した場合、前記保持した前記コンテンツ複製要求と、IPアドレスと、S2205における判定結果とに基づき前記要求管理情報を生成し前記管理要求キューに繋ぐ(S2206)。

#### 【0351】

前記配信装置は、S2206において繋いだ前記要求管理情報がキューの先頭になるのを待つ(S2207)。

前記配信装置は、前記要求管理情報がキューの先頭になった場合、前記要求管理情報に基づきコンテンツの複製処理を再開する。

配信装置は、前記要求管理情報中のグループ内外情報と、前記装置属性情報とに基づき、対象残数を選択し、前記対象残数が0であるか否かを判定する(S2208)。

30

#### 【0352】

前記対象残数は、グループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数から選択した1の残数である。

前記グループ内外情報がグループ内を示し、前記装置属性情報が装置を示す場合、前記対象残数はグループ内装置残数である。

同様に、前記グループ内外情報がグループ外を示し、前記装置属性情報が装置を示す場合、前記対象残数はグループ外装置残数である。

#### 【0353】

前記グループ内外情報がグループ内を示し、前記装置属性情報が媒体を示す場合、前記対象残数はグループ内媒体残数である。

40

前記グループ内外情報がグループ外を示し、前記装置属性情報が媒体を示す場合、前記対象残数はグループ外媒体残数である。

前記対象残数が0である場合(S2208: YES)、前記配信装置は、複製不可を示す複製可否通知を、前記要求装置に送信し処理を終了する(S2209)。

#### 【0354】

前記要求装置は、複製不可を示す複製可否通知を配信装置から受信したか否かを判定する(S2210)。

前記複製可否通知を受けたと判定した場合(S2210: YES)、要求装置は処理を終了する。

50

前記対象残数が0でない場合（S2208：NO）、前記配信装置は、コンテンツをセッション鍵で暗号化し（S2211）、配信装置へ送信する（S2212）。

【0355】

前記要求装置は、受信した前記暗号化されたコンテンツをセッション鍵を用いて復号化し、記憶部2207に保持する（S2213）。

前記要求装置は、前記配信装置に対し、コンテンツ複製完了通知を送信する（S2214）。

前記配信装置は、前記コンテンツ複製完了通知を受信し、前記対象残数を1減少させる（S2215）。

【0356】

配信装置は、前記要求管理キューの先頭の前記要求管理情報を削除し、前記要求管理キューを更新する（S2216）。

#### 4. 3. 4 複製制限管理情報譲渡処理

前記配信装置が、管理している前記複製制限管理情報を他の装置に譲渡することにより、前記他の装置が前記コンテンツの複製を許可する権限を持つこととなる。

【0357】

図46は、複製制限管理情報譲渡処理を示すフローチャートである。

ここでは、要求装置は再生装置2002であり、配信装置はホームサーバ2001であり、他装置は再生装置2003であるものとする。

前記要求装置は、まずネットワーク上で、複製数の譲渡元となる装置が複数稼働している場合に、いずれの装置に譲渡を要求するかを決定する。

【0358】

前記要求装置は、所望のコンテンツを識別するコンテンツ確認情報と、譲渡を希望する複製要求数を含む複製数譲渡要求を、ネットワーク上にブロードキャスト送信する（S2301）。

前記複製要求数は、8桁の数字であり、上から2桁がグループ内装置残数、上から3、4桁目がグループ外装置残数、上から5、6桁目がグループ内媒体残数、上から7、8桁目がグループ外媒体残数であるとする。

【0359】

例えば、譲渡を要求するグループ内装置残数が80、グループ外装置残数が2、グループ内媒体残数が50、グループ外媒体残数が3である場合、前記複製要求数は、80025003となる。

前記配信装置は、ブロードキャストされた前記コンテンツ確認情報で識別されるコンテンツを管理し、かつ、前記複製要求数に含まれる各残数以上のグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数を保持している場合、譲渡可と判定し、それ以外の場合譲渡不可と判定する（S2302）。

【0360】

前記配信装置は、譲渡不可であった場合（S2302：NO）、処理を終了する。

同様に、前記他装置は、ブロードキャストされた前記コンテンツ確認情報で識別されるコンテンツを管理し、かつ、前記複製要求数に含まれる各残数以上のグループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数を保持している場合、譲渡可と判定し、それ以外の場合譲渡不可と判定する（S2303）。

【0361】

前記他装置は、譲渡不可であった場合（S2303：NO）、処理を終了する。

前記配信装置は、譲渡可であった場合（S2302：YES）、譲渡可を示す譲渡可否通知を前記要求装置に送信する（S2304）。

前記他装置は、譲渡可であった場合（S2303：YES）、譲渡可を示す譲渡可否通知を前記要求装置に送信する（S2305）。

【0362】

前記要求装置は、受信した各譲渡可否通知の内容を確認し、譲渡可を示す譲渡可否通知

10

20

30

40

50

の装置の送信元 IP アドレスを保持する (S 2306)。

前記要求装置は、前記保持した IP アドレスを持つ各装置に対し、ICMP エコーメッセージを送信し、前記送信の応答である ICMP エコーリプライメッセージを受信するまでの各応答時間を測定する。

【0363】

前記要求装置は、前記配信装置に対し、ICMP エコーメッセージを送信する (S 2307)。

前記配信装置は、ICMP エコーメッセージを受信し、応答として前記要求装置に対し、ICMP リプライメッセージを送信する (S 2308)。

前記要求装置は、ICMP エコーリプライメッセージを受信し、応答時間を計算する。 10

【0364】

前記要求装置は、他装置に対し、ICMP エコーメッセージを送信する (S 2309)。

前記他装置は、ICMP エコーメッセージを受信し、応答として要求装置に対し、ICMP エコーリプライメッセージを送信する (S 2310)。

前記要求装置は、ICMP エコーリプライメッセージを受信し、応答時間を計算する。

【0365】

前記要求装置は、譲渡元装置として、応答時間の最短であった装置を選択する (S 2311)。

前記要求装置は、前記譲渡元装置の IP アドレスを保持しておく。 20

ここで、前記要求装置は、前記譲渡元装置として、前記配信装置を選択したものとす

【0366】

前記要求装置と前記配信装置は、図 43 及び図 44 に示す相互認証と鍵共有を行う (S 2312)。

配信装置と、要求装置とは、S 2312 の実行結果としてセッション鍵を共有する。

前記セッション鍵の共有が完了以後は、配信装置と要求装置との間の通信は、前記セッション鍵を用いて暗号化復号化される。

【0367】

前記要求装置は、前記配信装置に対し、前記グループ所属情報と、前記複製要求数とを送信する (S 2313)。 30

前記配信装置は、受信した前記グループ所属情報と、認証部 2103 で保持しているグループ所属情報とが一致しているか否かを確認し、一致している場合グループ内であり、一致しない場合グループ外と判定する (S 2314)。

【0368】

前記配信装置は、グループ内と判定した場合 (S 2314: YES)、複製制限情報管理部 2102 に保持している、グループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数から、前記複製要求数が示す各残数を引く (S 2315)。

例えば、前記配信装置が保持するグループ内装置残数が 99、グループ外装置残数が 10、グループ内媒体残数が 99、グループ外媒体残数が 10 であり、前記複製要求数が値「30051001」の場合、S 2315 を実行したのち、前記配信装置は、グループ内装置残数として値「69」、グループ外装置残数として値「5」、グループ内媒体残数として値「89」、グループ外媒体残数として値「9」を保持することとなる。 40

【0369】

前記配信装置は、譲渡複製数を、値「30051001」とする。

グループ外であった場合 (S 2314: NO)、前記譲渡複製数を値「0」とする。

前記配信装置は、前記譲渡複製数と、保持している前記使用期限情報を含む譲渡許可通知を前記要求装置に送信する (S 2316)。

前記要求装置は、受信した前記譲渡複製数が 0 か否かを判定する (S 2317)。

【0370】

前記譲渡複製数が0であった場合（S2317：YES）、要求装置は処理を終了する。

前記譲渡複製数が0でなかった場合、要求装置中の複製制限情報管理部2202は、前記コンテンツ確認情報をコンテンツ識別子とし、前記コンテンツ識別子と譲渡複製数と前記使用期限情報とを対応づけて、複製制限管理情報として保持する（S2318）。

#### 4. 3. 5 使用期限管理処理

予め使用期限の定められたコンテンツを、配信装置から、要求装置へ複製した場合の処理について説明する。

##### 【0371】

前記配信装置、前記要求装置それぞれが備える時計が前記使用期限を示す時刻に到達した場合、前記要求装置は前記コンテンツの消去を行い、前記配信装置は、前記消去したコンテンツに対応した複製許可の残数を増やす処理を行う。

10

図47は、使用期限の定まったコンテンツを管理する使用期限管理処理を示す。

図47中、配信装置はサーバ2001であるとし、要求装置は、再生装置2002であるとする。

##### 【0372】

前記配信装置は、前記要求装置との間で、図45に示したように、コンテンツの複製を行う（S2401）。

前記配信装置は、S2212における、前記要求装置へのコンテンツの送信時に、前記使用期限情報を送信するものとする。

20

前記要求装置は、受信した前記使用期限情報を保持する。

##### 【0373】

前記配信装置は、時間管理部2105に対し、時間管理部2105中の時計が前記使用期限情報を刻んだ場合に通知するよう指示する（S2402）。

前記要求装置は、時間管理部2205に対し、時間管理部2205中の時計が前記使用期限情報を刻んだ場合に通知するよう指示する（S2402）。

前記配信装置は、時間管理部2105からの前記通知があった場合（S2402：YES）、前記要求装置に対応する残数を、1増加させる（S2403）。

##### 【0374】

例えば、前記要求装置が、グループ内の装置である場合には、前記複製制限管理情報中のグループ内装置残数を1増加させ、前記要求装置がグループ外の装置である場合には、前記複製制限管理情報中のグループ外装置残数を1増加させる。

30

前記要求装置は、時間管理部2205からの前記通知があった場合（S2404：YES）、前記使用期限情報に対応する前記コンテンツを消去する（S2405）。

#### 4. 3. 6 複製予約実行処理

図48は、コンテンツの複製予約実行処理を示す図である。

##### 【0375】

配信装置、要求装置、他装置は、それぞれ、図42に示すコンテンツ複製元決定処理を行う（S2501）。

ここで、前記配信装置はホームサーバ2001、前記要求装置は、再生装置2002、前記他装置は、再生装置2003であるとする。

40

前記要求装置は、S2501により、複製元として、前記配信装置を選択したものである。

##### 【0376】

前記配信装置は、S2501中で取得した、複製を希望するコンテンツを識別するコンテンツ確認情報を保持しておく。

前記要求装置は、前記配信装置に対し、前記複製を実際に開始する複製開始時刻を含む複製予約要求を送信する（S2502）。

前記配信装置は、前記複製予約要求を受信し、時間管理部2105に、前記複製開始時刻になった場合を検出するようタイマー設定する（S2503）。

50

## 【0377】

前記配信装置は、時間管理部2105において、前記複製開始時刻になったことを検出する(S2504)。

前記要求装置と、前記配信装置とは、図45のS2203以降の処理を実行し、コンテンツの複製を行う(S2505)。

## 4.3.7 コンテンツ返却処理

配信装置から要求装置へコンテンツの複製を行った後、前記要求装置側で前記コンテンツの消去を実行し、前記配信装置側で、前記要求装置側での前記消去に対応する残数を1増加させ前記コンテンツを複製出来る残数を1増やすことをコンテンツ返却処理と称す。

## 【0378】

図49は、コンテンツ返却処理を示すフローチャートである。

ここで、前記要求装置は再生装置2002であり、前記配信装置はホームサーバ2001であるとする。

また、前記配信装置は、前記要求装置に対して、コンテンツを複製しているものとする。

## 【0379】

前記要求装置は、前記配信装置に対し、返却するコンテンツを識別するコンテンツ確認情報を含む、コンテンツ返却要求を送信する(S2601)。

前記配信装置は、受信したコンテンツ返却要求を保持する。

前記要求装置と、前記配信装置とは、図43及び図44に示した相互認証と鍵共有処理を実行する(S2602)。

## 【0380】

前記要求装置は、S2602を実行することにより、前記配信装置とセッション鍵を共有する。

前期要求装置は、前期配信装置に対し、前記グループ所属情報を送信する(S2603)。

前記配信装置は、前記受信したグループ所属情報と、自身が保持しているグループ所属情報とが一致するか否かを調べ、一致する場合、前記要求装置がグループ内であると判定し、一致しない場合は、前記要求装置がグループ外であると判定する(S2604)。

## 【0381】

前記要求装置がグループ外であった場合(S2604:NO)、前記配信装置は、前記要求装置にエラー通知を送信し(S2605)、処理を終了する。

前記要求装置は、前記エラー通知を受信した場合(S2606:YES)、処理を終了する。

前記要求装置がグループ内であると判定した場合(S2604:YES)、前記要求装置は、前記コンテンツ返却要求を形式変換して前記要求管理情報として要求管理キューにキューイングする(S2607)。

## 【0382】

前記配信装置は、前記コンテンツ返却要求に係る前記要求管理情報が、要求管理キューの先頭になるのを検出する(S2608)。

前記コンテンツ返却要求が要求管理キューの先頭になった場合(S2608:YES)、前記配信装置は、前記コンテンツ確認情報を含む返却処理開始通知を、要求装置に対し送信する(S2609)。

## 【0383】

前記返却処理開始通知を受信した要求装置は、前記返却処理開始通知に含まれるコンテンツ確認情報が識別するコンテンツを消去する(S2610)。

前記要求装置は、前記配信装置に対し、前記コンテンツ確認情報を含むコンテンツ消去完了通知を送信する(S2611)。

前記配信装置は、前記消去に対応する前記対象残数を1増加させる(S2612)。

## 【0384】

10

20

30

40

50

前記配信装置は、前記要求管理キュー先頭から、前記コンテンツ返却要求を削除し、前記要求管理キューを更新する（S2613）。

#### 4. 4 変形例

(1) 媒体は、装置を介して、ホームサーバに接続しているが、ホームサーバに媒体挿入口を設け、挿入口に挿入された媒体と、ホームサーバとを接続し、相互に認証、コンテンツのコピー等を行ってもよい。

##### 【0385】

媒体と、ホームサーバとの間に再生装置とネットワークとを介するのと、直接接続するとの違いであり、相互の認証、コンテンツの複製等の方法に違いは生じない。

(2) コンテンツ配布元決定部2206は、コンテンツの配布元を決定するために、ICMPエコーメッセージとICMPエコーリプライメッセージとを用いなくてもよい。 10

コンテンツ配布元決定部2206は、各装置の情報処理能力を予め記憶しておき、ブロードキャストに対し応答してきた装置の中で、情報処理能力の一番高い装置をコンテンツの配布元と決定してもよい。

##### 【0386】

また、コンテンツ配布元決定部2206は、各装置の優先度を予め設定し、ブロードキャストに対し応答してきた装置の中で、最も優先度の高い装置を前記コンテンツの配布元としてもよい。

(3) 複製管理情報は、使用期限情報を含んでいるが、その他の情報を用いて、コンテンツの複製制限を加えてもよい。 20

##### 【0387】

例えば、複製制限情報管理部は、地域制限情報を保持していてもよい。

前記地域制限情報は、前記コンテンツを複製してもよい地域を示す情報である。

前記地域制限情報は、値として、例えば、日本を示す値「1」、米国を示す値「2」、ドイツを示す値「3」を取りうるものとする。

前記地域制限情報の値が「1」であった場合は、コンテンツの複製を、日本国内にある装置に対してのみに制限する。

##### 【0388】

また、複製制限情報管理部は、リボケーションリストを保持していてもよい。

前記リボケーションリストは、前記コンテンツの複製の許可が与えられない装置を示すリストである。 30

前記リボケーションリストが示す装置に対しては、複製制限情報管理部2102は、前記コンテンツの複製許可を与えない。

##### 【0389】

また、複製制限情報管理部は、複製世代情報を保持していてもよい。

前記複製世代情報は、コンテンツの再度の複製を何回許すかを示す。

例えば、前記複製世代情報が2であるコンテンツは、いわゆる、子コピーと孫コピーまでが許可されることとなる。

(4) コンテンツ複製管理システムは、課金システムと協働してもよい。

##### 【0390】

本システムが、グループ外装置に対し、コンテンツの複製許可を与えると判断した場合に、課金システムに対し、課金依頼を送信する。 40

前記課金依頼には、コンテンツの利用者と、課金金額が含まれる。

前記課金システムは、予め、コンテンツの利用者と契約を行い、課金が発生した場合の、例えばクレジットカードを用いて精算する等の契約を行っている。

##### 【0391】

精算処理が滞りなく実施された場合に、前記課金システムは、サーバに対し、精算処理の終了を通知する。

精算処理の終了通知を受け、前記サーバは、要求装置に対し、コンテンツの複製許可を与えた後、コンテンツの複製を行う。 50

あるいは、家庭内ネットワークの中であっても、コンテンツの複製が行われるたびに、課金してもよい。

【0392】

(5) 実施形態中で、再生装置2002が、ホームサーバ2001から、コンテンツの複製を許可する権利の譲渡を受ける形態について説明したが、再生装置2002は、ホームサーバ2001が稼動できなくなった場合にバックアップ機として稼動することとしてもよい。

(6) 複製管理情報として、装置に関して前記グループ内装置残数と、前記グループ装置残数とを管理し、記憶媒体に対して前記グループ内媒体残数と、前記グループ外媒体残数とを管理しているが、管理上、前記装置と前記記憶媒体とを区別せず、前記グループ内装置残数と前記グループ内媒体残数との合計数をグループ内許可残数として管理し、前記グループ外装置残数と前記グループ外媒体残数との合計数をグループ外許可残数として管理してもよい。

【0393】

(7) ホームサーバは、ネットワークを通じて複製制限情報を放送とは別に取得することとしているが、取得経路はネットワークに限るものではない。

放送局が放送により複製制限情報を送信し、ホームサーバが当該放送を受信することにより前記複製制限情報を取得することとしてもよい。

(8) コンテンツ複製元決定処理において、要求装置は、コンテンツ確認要求をネットワーク上にブロードキャスト送信しているが、ブロードキャスト以外を用いてもよい。

【0394】

例えば、所望のコンテンツの配布元となりうる装置の候補が予め定められている場合には、要求装置は、コンテンツ確認要求を、マルチキャスト送信してもよい。

(9) 複製制限情報管理部は、要求管理キューに繋がれた要求管理情報について、前記要求管理キューの先頭に繋がれた要求管理情報に対する処理を行っているが、キューの先頭に繋がれた要求管理情報に係る残数(グループ内装置残数、グループ外装置残数、グループ内媒体残数、グループ外媒体残数のうちのいずれか)が0であり処理区分で示される処理が出来ない場合に、キューの先頭以外に繋がれた要求管理情報であって、処理区分が消去を示す要求管理情報を先に処理してもよい。

【0395】

複製制限情報管理部は、処理区分が消去である要求管理情報を優先して処理することにより前記残数が1増加するため、キューの先頭に繋がれた要求管理情報に関する処理を行うことが出来る。

## 5. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのももちろんである。以下のような場合も本発明に含まれる。

(1) 本実施の形態で、AD内サーバ100と接続されていない機器を登録する際に、ICカード400を用いてCSIをコピーするとしたが、クライアント機器間でCSIを移動することとしてもよい。

【0396】

再生装置200から再生装置200nにCSIを移動し、再生装置200nをAD内機器として登録する際を例として説明する。

再生装置200と再生装置200nとを接続し、再生装置200nを操作して移動通知を再生装置200に送信する。再生装置200及び再生装置200nは、SACを確立してセッション鍵SKを生成する。再生装置200は、セッション鍵SKでCSIを暗号化して再生装置200nへ送信する。再生装置200nは、セッション鍵を用いて暗号化CSIを復号して格納し、SAC確立の際に受け取った移動元である再生装置200のIDを記憶する。また、再生装置200へ受領通知を送信する。再生装置200は、受領通知を受信すると、CSI格納部208のCSIを削除して、「0」を格納する。

【0397】

10

20

30

40

50



再生装置 200n は、A D 内サーバ 100 に接続され、S A C を確立すると、A D 内サーバ 100 に C S I を移動されたことを通知し、移動元の I D 及び再生装置 200n の I D を送信し、A D 内サーバ 100 は、登録情報の機器 I D を書き換える。

(2) I C カード 400 は A D 内サーバ 100 に付属の機器であるとしたが、付属でなくとも良い。

【0398】

I C カード 400 も他のクライアント機器と同様に、A D 内サーバ 100 に接続されると S A C を確立し、I D — 4 を機器 I D として登録し、C S I を取得する。

A D 内サーバ 100 は、D V D 500 にコンテンツ鍵を記録する際、コンテンツ鍵を I C カード 400 の I D — 4 と C S I とを連結して生成した暗号鍵を用いて暗号化する。

車載機器 300 は、D V D 500 が装着され、I C カード 400 が接続されると、I C カード 400 との間で S A C を確立してセッション鍵を共有する。

【0399】

I C カード 400 は、I C カード 400 内に記憶している I D — 4 と C S I とを連結して復号鍵を生成し、セッション鍵 S K を用いて復号鍵を暗号化して暗号化復号鍵を生成して車載機器 300 へ送信する。

車載機器 300 は、暗号化復号鍵をセッション鍵 S K を用いて復号して復号鍵を生成し、D V D から読み出す暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、コンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを再生する。

【0400】

また、上記(1)のように、クライアント間で C S I を移動する場合と同様の処理を行い、I C カードから車載機器 300 に C S I を移動しても良い。この場合、実施の形態 1 の I C カード 400 と同様に、付属でない I C カードに、A D 内サーバ 100 へ移動を通知する機能を持たせても良い。車載機器 300 に C S I を移動した I C カードは、その場で C S I を削除せずに、C S I の移動を禁止し、A D 内サーバ 100 に移動を通知した後 C S I を削除する。

(3) I C カード 400 を用いて A D 内サーバ 100 に接続されていない機器を登録する場合、ネットワークを介して A D 内サーバ 100 から I C カード 400 に許可権利又は C S I を送信するとしても良い。

【0401】

一例として、P C などネットワークに接続して通信する機能を有するクライアント機器に、I C カード 400 が接続されると、I C カード 400 は、P C の通信機能を利用して、S A C 確立の処理を行い、許可権利又は C S I を受信する。

通信機能を有するクライアント機器は、P C に限らず、P D A や携帯電話などであっても良い。

(4) 本実施の形態では、A D 内サーバ 100 からクライアント機器へコンテンツを配送、又は D V D に記録して配布するとしたが、クライアント機器間で S A C を確立してセッション鍵 S K を生成し、コンテンツを配送するとしても良い。

(5) 本実施の形態で、I C カード 400 を用いて車載機器 300 を登録するとしたが、同様に I C カード 400 を用いて、脱退の処理を行っても良い。

【0402】

この場合、I C カード 400 を接続された車載機器 300 を操作して、I C カード 400 へ脱退要求を送信し、I C カード 400 は、S A C を確立して車載機器 300 が登録済みであることを確認し、車載機器 300 へ削除通知を送信する。車載機器 300 は、C S I を削除し、I C カード 400 へ削除完了通知を送信する。I C カード 400 は、削除完了通知を受信すると、脱退した車載機器 300 の I D を記憶する。I C カード 400 は、A D 内サーバ 100 に接続されると、A D 内サーバ 100 に、車載機器 300 が脱退した旨と、車載機器 300 の I D とを通知する。A D 内サーバ 100 は、機器 I D から車載機器 300 の I D を削除し、登録台数から「1」減算し、残数に「1」を加算する。

(6) 本実施の形態で A D 内サーバ 100 は、S A C を確立する際の署名検証で相手機器

10

20

30

40

50

が格納しているＣＳＩの値によって、相手機器が未登録であるか登録済みであるかを確認するとしたが、認証する機器からＩＤを受信し、登録情報の機器ＩＤに、受信したＩＤが記憶されているか否かによって、未登録か、登録済みかを確認するとしても良い。また、ＡＤ内の機器として登録されているクライアント機器全てが、登録されているＩＤを記憶しており、クライアント機器間でも同様に、ＩＤによって、登録、未登録を確認するとしても良い。

(7) ＡＤ内サーバ１００と接続されていない機器を登録する際、ＩＣカード４００を用いるとしたが、ＡＤ内サーバ１００がＣＳＩを表示部１１４に表示し、それをユーザがクライアント機器に手入力するとしても良い。この場合、入力するコードは、機器やセッションに依存してＣＳＩを暗号化した値であっても良い。

(8) 本実施の形態で、ＳＡＣを確立し、ＣＳＩを暗号化して送信する際、暗号文に暗号化ＣＳＩを送信する機器の署名データを付加して送信するとしても良い。

(9) 本実施の形態で、登録情報及びＣＳＩは、それぞれの機器の内部に格納されるとしたが、着脱可能で、許可なく読み出し、書き込み及びコピーが出来ない領域に格納するとしても良い。

(10) 本実施の形態で、コンテンツを暗号化する際の暗号化鍵、又は復号する際の復号鍵として、機器のＩＤ及びＣＳＩ又は乱数及びＣＳＩを連結して利用するとしたが、この限りではなく、機器のＩＤ及びＣＳＩ又は乱数及びＣＳＩを用いて演算を行い、その結果得られる値を用いるとしても良い。

(11) 本実施の形態では、登録情報として、最大数、登録台数及び残数を管理するとしたが、これに限らない。

#### 【０４０３】

最大数を残数の初期値とし、登録する度に残数から「１」ずつ減らし、残数が「０」でなければクライアント機器を登録するとしてもよい。また、最大数と、登録台数とを管理し、登録台数が最大数以下であれば、クライアント機器を登録するとしても良い。

(12) 登録情報の機器の台数は、ＡＤ内サーバ１００とオンラインで接続している機器と、ＩＣカード４００を用いて登録する機器とを分けて、最大数、登録台数などを管理しても良い。

(13) 本実施の形態では、ＡＤ内サーバ１００が記憶している登録情報を基に管理しているが、別途管理機関を設け、以下(α)～(c)のようにしても良い。

#### 【０４０４】

(α) 管理機関が最大数を設定し、最大数に管理機関の署名データを付して、ＤＶＤなどの可搬型の記録媒体に記録して配布、又は通信を介して配布する。ＡＤ内サーバ１００は、署名データを検証し、検証結果が成功の場合に、最大数として記憶する。

(b) ＡＤ内サーバ１００は、登録したい台数を管理機関に要求する。管理機関は、台数に応じた課金を行い、課金に成功した場合に、要求した台数の登録を許可する情報をＡＤ内サーバ１００へ送信し、ＡＤ内サーバ１００は情報を受け取ると、許可された台数の範囲内でクライアント機器の登録を受け付ける。

#### 【０４０５】

(c) ＡＤ内サーバ１００は、クライアント機器からの登録を受け付ける度に、管理機関に要求を出し、管理機関は、要求に対して課金を行い、課金に成功すると、登録を許可する。ＡＤ内サーバ１００は、許可されると、クライアント機器を登録し、ＣＳＩを送信する。

(14) 再生装置２００は、ＡＤ内サーバ１００から配送されたコンテンツを再生するとしたが、ＤＶＤ再生機能を有し、ＡＤ内サーバ１００によってＤＶＤ５００に記録されたコンテンツを再生するとしても良い。

#### 【０４０６】

また、ＡＤ内サーバ１００は、登録情報に記憶している機器ＩＤ全てを、それぞれＣＳＩと連結してコンテンツ鍵の暗号化に用いるとしたが、ＤＶＤを再生する機能を有する機器のＩＤを予め記憶しており、ＤＶＤを再生できる機器のＩＤを抽出し、それぞれＣＳＩ

10

20

30

40

50

と連結してコンテンツ鍵の暗号化に用いるとしても良い。

(15) 本実施の形態では、A D内サーバ100はD V Dにコンテンツを記録するとししたが、メモリーカード、M D、M O、C D、B D (B l u e r a y D i s k) などに記録するとしても良いし、I Cカードにコンテンツを記録するとしても良い。

【0407】

また、クライアント機器は、再生装置の他、記録装置でもよく、それらを組み合わせたものであってもよい。また、クライアント機器は、ユーザ宅内に設置されている又は車両に搭載されている他、ユーザが持ち運ぶことができる携帯型の機器であっても良い。

(16) I Cカード400は、A D内サーバ100又は車載機器300に直接接続されるため、S A Cの確立処理を行わなくても良い。

10

(17) S A C確立の際、乱数C h a - B又はC h a - Aに、C S Iを連結したデータに対して署名データ生成するとししたが、署名対象と成るデータのハッシュ値を計算し、このハッシュ値に対して署名データを生成するとしても良い。

(18) S A C確立の際、認証相手の機器が未登録か登録済みかを判断するとき及び鍵共有のときにC S I利用するとししたが、どちらか一方に利用するとしても良い。

【0408】

また、本実施の形態では双方向に認証を行っているが、片方向認証であっても良い。

(19) クライアント機器の登録を、時間で制限するとしても良い。

A D内サーバ100とクライアント機器との間で時間を合わせる。A D内サーバ100は、C S Iの使用を許可する期間を設定して有効期限情報とし、有効期限情報とC S Iとをクライアント機器に送信し、登録台数から「1」減算する。

20

【0409】

クライアント機器は、有効期限情報及びC S Iを受信し、格納する。有効期限情報が示す期間が終了すると、C S Iを削除する。

A D内サーバ100は、有効期限情報が示す期間が終了すると、登録台数に「1」を加算する。機器I Dを記憶している場合は、期限が切れた機器のI Dを削除する。

なお、有効期限情報は、有効期限の開始と終了の日時を示す情報でも良いし、終了の日時のみ示すものであっても良い。また、C S Iの使用開始からの期間を制限するものであっても良いし、C S Iを使用してクライアント機器が動作している期間を制限するとしても良い。

30

(20) 本実施の形態では、A D内サーバは1つであるとして説明したが、一つのA Dに複数のA D内サーバがあっても良い。

【0410】

この場合、クライアント機器は、何れのA D内サーバと通信するかを選択することが出来る。選択方法として、ユーザが設定するとしても良いし、クライアント機器がA D内で、当該クライアントと距離が最短のA D内サーバを選択しても良い。また、A D内サーバのうち、処理能力が高いものや、他のタスクが少ないA D内サーバを選択するとしても良い。

【0411】

また、以下のように、クライアント機器から登録を要求されたA D内サーバが、それ以上クライアント機器を登録出来ない場合、登録可能な他のA D内サーバを探すとしても良い。

40

クライアント機器は、1つのA D内サーバに登録要求を送信する。登録要求を受信したA D内サーバは、登録台数が最大数と一致する場合、他のA D内サーバに、クライアント機器を登録できるか問い合わせる。他のA D内サーバは、登録可能である場合、要求元のクライアント機器を登録し、A D内サーバに登録可能である旨を応答し、A D内サーバは、クライアント機器へC S Iを送信する。

【0412】

また、他のA D内サーバが登録できない旨を応答した場合、A D内サーバは、更に他のA D内サーバへ問い合わせる。

50

また、複数のAD内サーバ間で代表となるAD内サーバを決定し、代表サーバが全てのグループ内機器を管理するとしても良い。この場合、代表でないAD内サーバがクライアント機器から登録要求を受け付けると、代表サーバに登録可能であるか問い合わせ、登録可能である場合、クライアント機器は代表サーバに登録され、代表サーバから要求を受け付けたAD内サーバを介してC S Iを受け取る。

【0413】

なお、要求を受け付けたAD内サーバが、他の処理を行っている場合などに、他のAD内サーバへ問い合わせるとしても良い。

また、以下(a)、(b)のように、複数のAD内サーバ間で、登録した機器の台数を管理するために、登録した機器に関するリストを共有するとしても良い。

(a) 同一AD内のAD内サーバR及びAD内サーバSはそれぞれ、クライアント機器に登録すると、登録した機器のIDを機器リストとして記憶する。また、IDを書き込むことでリストが更新される度に、バージョン番号を機器リストに対応付けて記憶する。

【0414】

AD内サーバR及びSは、定期的又は不定期に前記機器リストを交換する。AD内サーバRは、自分が記憶している機器リストのバージョン番号と、AD内サーバSから受け取った機器リストのバージョン番号とを比較し、より新しい方を機器リストとして記憶する。AD内サーバSも同様に処理する。これにより、常に最新の機器リストを共有することが出来る。

【0415】

なお、一方のAD内サーバの機器リストが更新されるたびに機器リストを交換するとしても良い。また、機器リストだけでなく、登録台数、最大数など、登録情報も、上記と同様に共有するとしても良い。

(b) 同一AD内のAD内サーバT及びAD内サーバUはそれぞれ機器リストT及び機器リストUを保持しており、それぞれクライアント機器に登録する際、機器IDと登録した時刻とを対応付けて格納する。AD内サーバT及びAD内サーバUは、定期的又は不定期に機器リストを交換する。

【0416】

AD内サーバTは、自分が登録情報として記憶している登録台数が最大数より少なければ、AD内サーバUから受け取った機器リストUに、新しく登録されたクライアント機器を、登録された順に、自分が保持している機器リストTに書き込む。また、AD内サーバUも同様に、機器リストTを受け取り、新しく登録された順に機器リストUを更新する。

なお、予めクライアント機器に優先順位を付しておき、優先順位が高い機器を優先的に登録するとしても良い。また、AD内サーバT及びUに新しく登録されたクライアント機器を合わせると最大数を超える場合、優先順位の高い機器を優先的に登録するとしても良いし、ユーザが登録する機器を選択しても良い。

【0417】

この方法によると、一方のAD内サーバが電源を切っていても、他方のAD内サーバに登録でき、他方のAD内サーバが更新されると、機器リストを交換して整合性を保つので、AD内サーバ間で同一の機器リストを共有することが出来る。

(21) 各ADのC S Iの重複を回避するために、それぞれのADを管理するAD内サーバ間で情報を交換して、重複しているか否かを確認するとしても良い。

【0418】

また、安全性を高めるために、AD内サーバは、それぞれのC S Iをハッシュ関数に入力してハッシュ値を算出し、ハッシュ値を交換して重複しているか確認するとしても良い。

また、AD内サーバがC S Iを生成する代わりに、管理機関を設けて、管理機関が全てのADのC S Iを重複しないように生成し、各AD内サーバに安全に送付するとしても良い。

(22) クライアント機器は複数のADに属するようにしてもよい。

## 【0419】

また、クライアント機器が、格納できるＣＳＩの数を制限すること、登録出来るＡＤの数を制限するとしても良い。また、各ＡＤ内サーバが登録されているクライアント機器のリスト情報を交換して、１つのクライアント機器が登録できるＡＤの個数を制限する構成であっても良い。また、リスト情報の交換により、クライアント機器がいくつのＡＤに属しているかを確認することが出来る。

## 【0420】

別途、クライアント機器が登録しているＡＤの数を管理する管理機関を設けても良い。

また、１台のＡＤ内サーバは、複数のＡＤを管理するとしても良い。この場合、ＡＤ内サーバは、それぞれ異なるＣＳＩを格納できる数を制限されており、この数以内のＡＤを管理できる。また、ＡＤ内サーバは、登録可能なクライアント機器の台数をＣＳＩ毎に記憶していても良いし、ＣＳＩとグループのＩＤとを対応付けて記憶するとしても良い。

(23) ＡＤは、それぞれ識別子を割り当てられており、コンテンツを配送する際に、コンテンツの配送元の機器は、当該機器が登録しているＡＤの識別子を電子透かしとしてコンテンツに埋め込むとしても良い。

## 【0421】

これにより、クライアント機器が復号したコンテンツを、不正にＡＤ外に配布した場合に、そのコンテンツがどのＡＤから流出したのかを特定することが出来る。更に、コンテンツの配信元のサーバが、各ＡＤに登録しているクライアント機器のＩＤを管理している場合、コンテンツを流出したクライアント機器のＩＤをＣＲＬに載せても良い。

(24) 本実施の形態では、機器の認証後にコンテンツを配送するとしたが、本発明はこれに限定されない。

## 【0422】

コンテンツを配送する際、以下のように、認証を行わないとしても良い。

コンテンツの送信側の機器は、ＣＳＩを基にして暗号鍵を生成する。生成した暗号鍵を用いてコンテンツ鍵を暗号化し、暗号化コンテンツと暗号化コンテンツ鍵とを配送する。

受信側の機器は、暗号化コンテンツと暗号化コンテンツ鍵とを取得すると、ＣＳＩを基にして、暗号鍵と同一の復号鍵を生成する。生成した復号鍵を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、コンテンツ鍵を用いて暗号化コンテンツを復号してコンテンツを生成する。

## 【0423】

これによると、ＣＳＩを保持する機器のみが復号鍵を生成し、コンテンツを復号することが出来る。

また、認証せずに、暗号化コンテンツのみ配送し、その後、実施の形態と同様に認証を行ってセッション鍵を共有し、認証に成功した場合に、セッション鍵でコンテンツ鍵を暗号化して配送するとしても良い。

## 【0424】

なお、暗号化コンテンツの配送は、通信で配送するとしても良いし、可搬型の記録媒体に記録して配布するとしても良い。

また、受信側の機器からの要求に応じてコンテンツを配送する他、要求がなくても送信側の機器が判断して配送するとしても良いし、外部からの入力に従って、配送するとしても良い。

(25) 本実施の形態で、ＣＳＩ格納部は、初期値として「０」を記憶しており、ＡＤ内サーバ１００が生成したＣＳＩを取得すると、取得したＣＳＩを上書きするとしたが、初期値とＣＳＩとを別の領域に記憶しても良い。また、取得したＣＳＩを初期値とは別の領域に記憶すると、初期値の使用を抑制するとしても良い。

## 【0425】

なお、使用を抑制した初期値は、移動、脱退などでＣＳＩを削除した際に、再度活性化される。

なお、未登録を示す値として「０」を格納するとしたが、「０」でなくとも良く、ＣＳ

10

20

30

40

50

Iとして生成される値と異なる値であればよい。

(26) 本実施の形態でA D内サーバ100はI Cカード400にC S Iのコピーを1回許可しているが、複数回の許可を与えても良い。

【0426】

また、I Cカード400は、C S Iを用いてクライアント機器を認証する他、C S Iをコピーしたクライアント機器のI Dを記憶しておき、コピーする際にクライアント機器のI Dを確認すること、同じクライアント機器へ複数回C S Iをコピーすること防ぐとしても良い。

また、クライアント機器の登録処理を行う機能をI Cカードに実装し、I Cカードを接続された機器がA D内サーバとして動作するとしても良い。

10

【0427】

また、クライアント機器が複数のクライアント機器の代表としてA D内サーバに登録し、他の複数のクライアント機器にC S Iをコピーする権利を受けるとしても良い。以下に、図50を用いて一例を示す。

ユーザ宅にはA D内サーバ600と、クライアント機器601とが設置されており、クライアント機器601は既にA D内サーバ600に登録されている。A D内サーバ600は、登録情報として最大と残数とを記憶しており、ここでは最大が4、残数が3であるとする。

【0428】

ユーザが所有する車両には、A D内サーバ600に登録されていない車載機器602、603、604が搭載されている。車載機器603、604は、A D内サーバ600と直接通信する機能を持たない。車載機器602は、可搬型でA D内サーバ600と直接通信する機能を有する。また、車載機器602～604は、それぞれ接続して通信可能である。

20

【0429】

車載機器602は、車載機器の代表として、A D内サーバ600に接続されると、登録したいクライアント機器の台数である希望台数3を含む登録要求をA D内サーバ600へ送信する。

A D内サーバ600は、登録要求を受信すると、実施の形態と同様に車載機器602を認証し、セッション鍵を共有する。認証に成功した場合、登録要求に含む希望台数が、登録情報として記憶している残数以下であるかを判断する。残数以下であると判断する場合、記憶しているC S Iを読み出し、読み出したC S Iと、3台分の登録を許可する許可権利とを、セッション鍵を用いて暗号化し、暗号化権利情報として車載機器602に送信する。

30

【0430】

車載機器602は、暗号化権利情報を受信すると、セッション鍵を用いて復号し、C S I及び許可権利を生成する。また、生成したC S Iを記憶すること、許可権利の内、1台分の許可権利を使ったので、残り2台登録できることを示す許可権利を記憶する。また、車載機器603及び604と、それぞれ認証を行い、成功するとC S Iを送信し、送信した台数分の許可権利を減らす。

40

【0431】

これによって、車載機器602～604をクライアント機器として登録できる。

なお、残数が希望台数未満である場合、残数が示す台数分だけ登録を許可する許可権利を送信する。例として、2台分の許可権利を送信した場合、車載機器602は、C S Iを記憶すること、1台分の許可権利を使い、車載機器603、604の何れかにC S Iを送信すること、もう1台分の許可権利を使う。C S Iの送信先の機器は、ユーザが選択するとしても良いし、それぞれの機器が予め優先順位を有し、優先順位の高い機器に送信するとしても良い。

【0432】

また、車載機器602～604をA D内サーバ600に登録する際、各車載機器のI D

50

をAD内サーバ600に登録する場合、以下のように処理する。

車載機器602は、登録する前に、車載機器603及び604のIDを取得する。AD内サーバ600に登録する際、取得したIDと、車載機器602自身のIDとをAD内サーバ600に送信する。AD内サーバ600は、受信したIDを機器IDとして記憶する。また、残数が希望台数未満である場合、AD内サーバ600は、受け取ったIDの内、残数が示す台数分のIDを記憶する。この場合、登録するIDをユーザが選択するとしても良いし、予めIDに優先順位を付し、優先順位の高いIDから順に残数が示す台数分のIDを記憶するとしても良い。

【0433】

また、車載機器602は、許可権利が余ると、AD内サーバ600に返すことが出来る。 10

なお、車載機器602は、当該車載機器602の権利を含めた許可権利を取得するとしたが、車載機器602は、実施の形態と同様にAD内サーバ600に登録し、車載機器603及び604にCSIをコピーする権利を取得するとしても良い。

(27)複数のADを合わせて1つのADを形成しても良い。

【0434】

一例として、AD-EとAD-Fとを合わせて、AD-Gを形成する場合を図51、を用いて説明する。

AD-E及びAD-Fは、それぞれ1台のAD内サーバと、図示していない複数のクライアント機器とから構成される。AD-EのAD内サーバEは、最大m台のクライアント機器が登録可能であり、AD-E内の機器は、それぞれCSI-Eを保持している。また、AD-FのAD内サーバFは、最大n台のクライアント機器が登録可能であり、AD-F内の機器は、それぞれCSI-Fを保持している。 20

【0435】

この2つのADからAD-Gを形成する。まず、AD内サーバEとAD内サーバFとの間で、AD-Gを管理するAD内サーバGとなる機器を決定する。この際、処理性能、各AD内サーバの優先順位などを基に決定しても良いし、ユーザが決定しても良い。AD内サーバGでない方のAD内サーバは、クライアント機器としてAD-Gに登録される。

AD内サーバGに登録可能な台数kは、m、n又はmとnとの平均とする。また、AD内サーバGは、新たにCSI-Gを生成して、各クライアント機器を認証し、認証に成功した機器へCSI-Gを送信する。 30

【0436】

AD-EとAD-Fとを形成する機器の合計が、台数kを超える場合、登録する機器が選択される。この場合、予め設定されている優先順位を下にAD内サーバGが選択しても良いし、ユーザが選択するとしても良い。

なお、上述のように、2つのADから新たに1つのADを形成するほか、一方のADに他方のADを足しても良い。AD-EにAD-Fを足す場合、AD-F内の機器はAD-Eのクライアント機器としてAD内サーバEに登録され、CSI-Eを保持する。この際、登録するクライアント機器の台数が最大m台を超える場合、上述のように、登録する機器が選択される。 40

【0437】

なお、m、n及びkは、正の整数である。

(28)1つのADから複数のADに分割するとしても良い。

一例として、AD-HからAD-IとAD-Jを形成する場合を、図52を用いて説明する。

AD-Hは、AD-H内の機器を管理するAD内サーバHと、図示していない複数のクライアント機器とから構成される。

【0438】

AD内サーバHは、P台(Pは正の整数)のクライアント機器が登録可能であり、AD-H内の各機器はCSI-Hを格納している。 50

A D内サーバHは、A D—I及びA D—Jを形成する際、A D—H内のクライアント機器から新たにA D内サーバI及びA D内サーバJとなる機器を選択する。この際、処理能力が高い機器をA D内サーバとしても良いし、予め各機器に付されている優先順位を基に選択しても良い。また、ユーザが選択しても良いし、クライアント機器間で処理能力、優先順位などを基に選択しても良い。なお、A D内サーバHがA D内サーバI又はA D内サーバJとして、新たなA Dを形成するとしても良い。

【0439】

分割後、それぞれに属するクライアント機器が選択される。この際、優先順位を基にそれぞれのA D内サーバが選択しても良いし、ユーザが選択しても良い。A D内サーバI及びJは、それぞれ最大P台のクライアント機器を登録可能である。また、各A Dのクライアント機器を選択すると、A D内サーバIは、C S I—Iを生成し、選択されたクライアント機器へ、生成したC S I—Iを送信する。また、A D内サーバJも同様に、C S I—Jを生成してクライアント機器へ送信する。

【0440】

なお、A D内サーバI及びJは、クライアント機器を選択する度に認証しても良いし、新たに生成したC S Iを送信する際に認証するとしても良い。

また、上記のように、1つのA Dから新たに2つのA Dを形成する他、A D—Hから新たなA Dを一つ形成し、基になったA D—Hと新たなA Dとの2つに分割するとしても良い。

(29) クライアント機器が電源を切ると、クライアント機器はA D内サーバに登録されたまま、C S Iは一旦削除されるとしても良い。

【0441】

この場合、クライアント機器がA D内サーバに登録されると、A D内サーバはクライアント機器のI Dを記憶し、C S Iを送信する。

クライアント機器は、受け取ったC S Iを記憶すると、A D内機器としてコンテンツを利用できる。クライアント機器は、電源OFFの指示を受け付けると、C S Iを削除し、電源をOFFにする。この際、A D内サーバが記憶しているクライアント機器のI Dは削除されない。

【0442】

再びクライアント機器の電源がONになると、クライアント機器は、A D内サーバにI Dを送信する。A D内サーバは、記憶しているI Dに、受信したI Dと一致するI Dが有るか否かを判断し、一致するI Dが有る場合、登録情報を更新せずに、クライアント機器にC S Iを再送信する。

なお、有線又は無線通信が遮断された場合も同様にC S Iを一旦消去し、通信が再度確立されると、I Dを送信し、C S Iを再度取得するとしても良い。

(30) 本実施の形態では、C S Iを用いて認証を行うとしたが、更に、以下の(a)～(c)の認証を追加しても良い。

【0443】

(a) M A CアドレスやI Pアドレス、またシステムで統一的に与えられたコードなどを用いてクライアント機器がA D内サーバと同一の家庭内LANに接続されていることを認証する。これにより、他人のクライアント機器を登録することが困難になる。

また、A D内サーバとクライアント機器とが無線で通信を行う場合、電波の届く範囲であることで認証しても良い。

【0444】

また、A D内サーバとクライアント機器とが通信可能な場合、A D内サーバからクライアント機器へ、認証用データを送信し、クライアント機器は、認証用データを受信すると、応答データをA D内サーバへ送信する。A D内サーバは、認証用データを送信してから応答データを受信するまでの時間を計時し、計時した時間が、予め設定している値以内であれば、同一宅内に設置されているものと認証するとしても良い。

【0445】

10

20

30

40

50



また、TTL (Time To Live) 値を宅内のルータの数以内に設定し、宅外の機器とは通信できないようにしても良い。

また、同じ電源に接続されているか否かを判断すること、同一宅内に設置されているか否かを認証するとしても良い。

(b) AD内サーバに予めパスワードを設定しておき、クライアント機器を登録する際、ユーザは前記パスワードをクライアント機器に手入力する。クライアント機器は入力されたパスワードを含む登録要求をAD内サーバへ送信し、AD内サーバは、登録要求に含んで受信したパスワードが、予め設定されたパスワードと一致するか否かを判断する。

【0446】

また、パスワードは複数設定しても良く、例えば家族それぞれが自分のパスワードを設定するとしても良い。また、ユーザそれぞれを識別するIDとパスワードとを組み合わせるとしても良い。

10

(c) 上記(b)におけるパスワードの代わりに、指紋や虹彩などのバイオメトリック情報を利用しても良い。これにより、予め設定した本人だけがクライアント機器の登録を行うことが可能となる。

(31) クライアント機器が保持している初期値は、以下(a)～(c)の場合がある。

【0447】

(a) クライアント機器は、AD内サーバに登録していないことを示す、1個の初期値を保持している。当該AD内サーバに登録されると、初期値の使用が抑制される。

(b) クライアント機器は、複数のAD内サーバそれぞれに対応する複数の初期値を保持している。複数のAD内サーバの何れかに登録する際、当該AD内サーバに対応する初期値を用いて認証し、登録されると、前記対応する初期値の使用を抑制する。また、他のAD内サーバに登録されると、他のAD内サーバに対応する初期値の使用を抑制する。

20

【0448】

なお、それぞれの初期値をグループの識別子に対応付けて識別しても良い。

(c) クライアント機器は、複数のAD内サーバの、何れにも登録していないことを示す初期値を保持している。何れかのAD内サーバに登録すると、初期値の使用を抑制する。

(32) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

30

【0449】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blue-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている

前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0450】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

40

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0451】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(33) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

50

【産業上の利用可能性】

【0452】

複製コンテンツの数を規制したコンテンツの管理に利用できる。

【図面の簡単な説明】

【0453】

【図1】グループ形成管理システム1の全体の構成を示すブロック図である。

【図2】AD内サーバ100の構成を示すブロック図である。

【図3】登録情報の構成を示す図である。

【図4】再生装置200の構成を示すブロック図である。

【図5】車載機器300の構成を示すブロック図である。

10

【図6】ICカード400の構成を示すブロック図である。

【図7】SAC確立の処理を示すフローチャートである。図8に続く。

【図8】SAC確立の処理を示すフローチャートである。図7の続き。

【図9】再生装置200をAD内サーバ100に登録する際の動作を示すフローチャートである。

【図10】車載機器300に登録する際の動作を示すフローチャートである。

【図11】車載機器300に登録する際の動作を示すフローチャートである。

【図12】コンテンツを配送する際の動作を示すフローチャートである。

【図13】コンテンツを配送する際の動作の一部を示すフローチャートである。

【図14】コンテンツをDVDに記録する際の動作を示すフローチャートである。

20

【図15】AD内サーバ100から脱退する際の動作を示すフローチャートである。

【図16】鍵配信システム1000を示すブロック図である。

【図17】コンテンツサーバ1001を示すブロック図である。

【図18】コンテンツ記憶部1011を示すブロック図である。

【図19】管理情報記憶部1012を示すブロック図である。

【図20】鍵情報記憶部1031が有する鍵情報テーブルT1001のデータ構造を示す

【図21】配信鍵情報記憶部1032が有する配信鍵情報テーブルT1002のデータ構造を示す。

【図22】記録媒体1002を示すブロック図である。

30

【図23】利用鍵記憶部1102が有する配信コンテンツ鍵テーブルT1101のデータ構造を示す。

【図24】再生装置1003を示すブロック図である。

【図25】再生装置1004を示すブロック図である。

【図26】コンテンツ鍵管理処理を示す流れ図である。図27へ続く。

【図27】コンテンツ鍵管理処理を示す流れ図である。図28から続く。

【図28】認証処理を示す流れ図である。

【図29】時間管理処理を示す流れ図である。

【図30】再生装置1004における再生時の動作を示す流れ図である。

【図31】再生装置1003における再生時の動作を示す流れ図である。

40

【図32】コンテンツサーバ1001にて記録媒体1002の利用時の動作を示す流れ図である。

【図33】コンテンツサーバ1001における再生時の動作を示す流れ図である。

【図34】鍵確認処理を示す流れ図である。

【図35】コンテンツ鍵の事前配信時の動作を示す流れ図である。

【図36】コンテンツ複製管理システム2000の構成を示すブロック図である。

【図37】ホームサーバ2001の構成を示すブロック図である。

【図38】複製制限情報管理部2102が保持する情報を示す。

【図39】再生装置2002の構成を示すブロック図である。

【図40】再生装置2003とIC内蔵可搬型記憶媒体2004との構成を示すブロック

50

図である。

【図４１】再生装置２００６の構成を示すブロック図である。

【図４２】コンテンツ複製元決定処理を示すフローチャートである。

【図４３】配信装置と要求装置との間で行われる相互の機器認証及び鍵共有の動作を示すフローチャートである。

【図４４】配信装置と要求装置との間で行われる相互の機器認証及び鍵共有の動作を示すフローチャートである。

【図４５】コンテンツの複製処理を示す図である。

【図４６】複製制限管理情報譲渡処理を示すフローチャートである。

【図４７】使用期限の定まったコンテンツを管理する使用期限管理処理を示す。

10

【図４８】コンテンツの複製予約実行処理を示す図である。

【図４９】コンテンツ返却処理を示すフローチャートである。

【図５０】複数のクライアント機器を、代表の機器がＡＤ内サーバに登録する場合の構成を示すブロック図である。

【図５１】複数のグループから一つのグループを形成する場合の概念を示す図である。

【図５２】一つのグループを分割して複数のグループを形成する場合の概念を示す図である。

【符号の説明】

【０４５４】

１ グループ形成管理システム

20

１０００ 鍵配信システム

１００１ コンテンツサーバ

Ｔ１００１ 鍵情報テーブル

１００２ 記録媒体

Ｔ１００２ 配信鍵情報テーブル

１００３ 再生装置

１００４ 再生装置

１００５ 再生装置

１００６ 放送局

１００７ ＧＷ

30

１０１１ コンテンツ記憶部

１０１２ 管理情報記憶部

１０１３ 利用鍵記憶部

１０１４ 受信部

１０１５ コンテンツ取得部

１０１６ 入力部

１０１７ 再生部

１０１８ 利用鍵監視部

１０１９ 利用鍵確認部

１０２０ 利用鍵事前配信部

40

１０２１ コンテンツ鍵制御部

１０２２ 認証部

１０２３ 時間管理部

１０２４ 入出力部

１０２５ 通信部

１０２６ 時計部

１０３１ 鍵情報記憶部

１０３２ 配信鍵情報記憶部

１１０１ コンテンツ記憶部

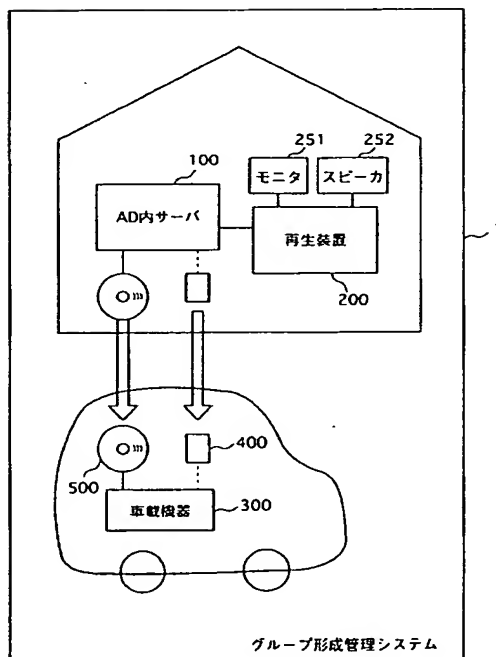
Ｔ１１０１ 配信コンテンツ鍵テーブル

50

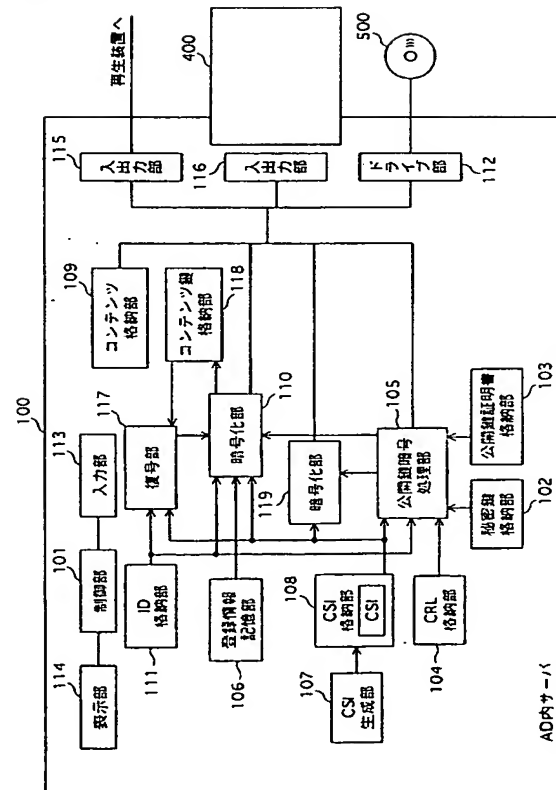
1 1 0 2	利用鍵記憶部
1 1 0 3	認証部
1 1 0 4	入出力部
1 2 0 1	入力部
1 2 0 2	再生部
1 2 0 3	利用鍵確認部
1 2 0 4	入出力部
1 2 0 5	通信部
1 2 0 6	時計部
1 3 0 1	コンテンツ記憶部
1 3 0 2	利用鍵記憶部
1 3 0 3	入力部
1 3 0 4	再生部
1 3 0 5	利用鍵監視部
1 3 0 6	認証部
1 3 0 7	通信部
1 3 1 0	時計部
1 3 1 1	時間管理部

10

【図 1】



【図 2】



【図 3】

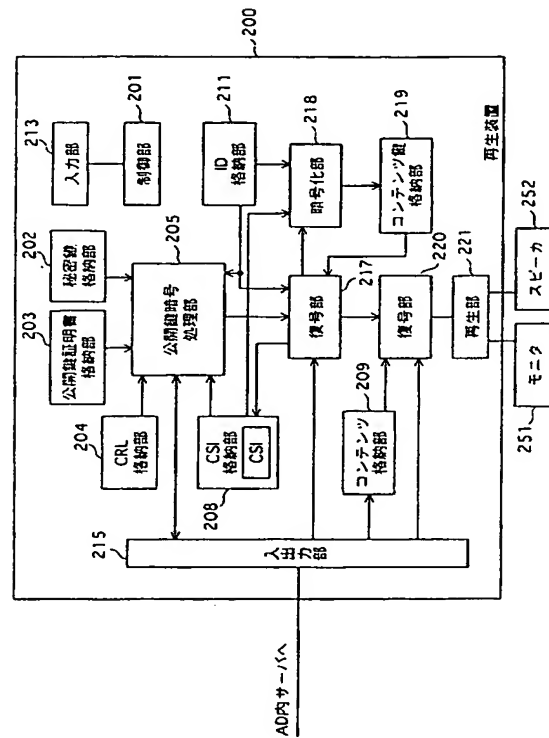
(a)

登録情報	
機器ID	
最大	2
登録台数	0
残数	2
ICカードID	ID_4

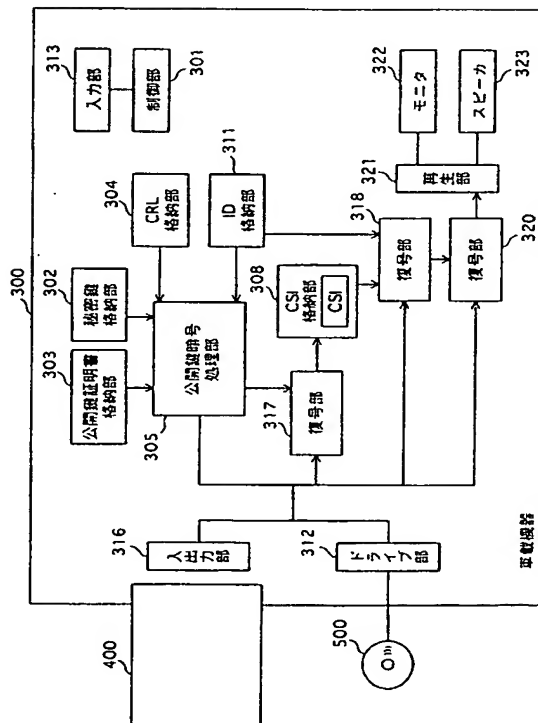
(b)

登録情報	
機器ID	ID_2
	ID_3
最大	2
登録台数	2
残数	0
ICカードID	ID_4

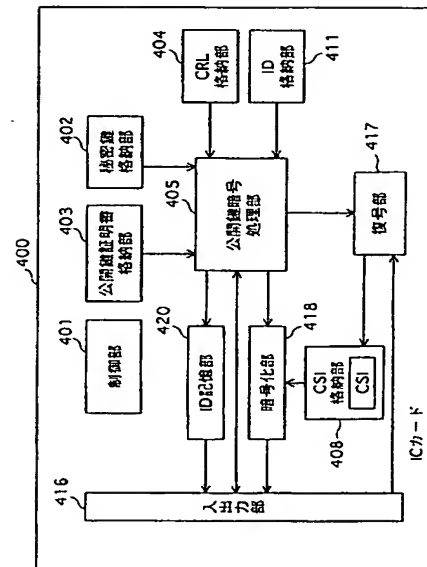
【図 4】



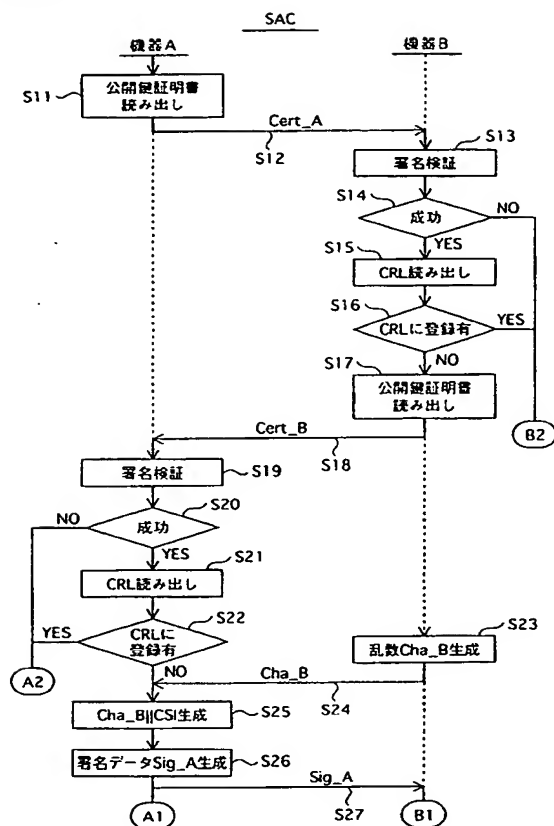
【図 5】



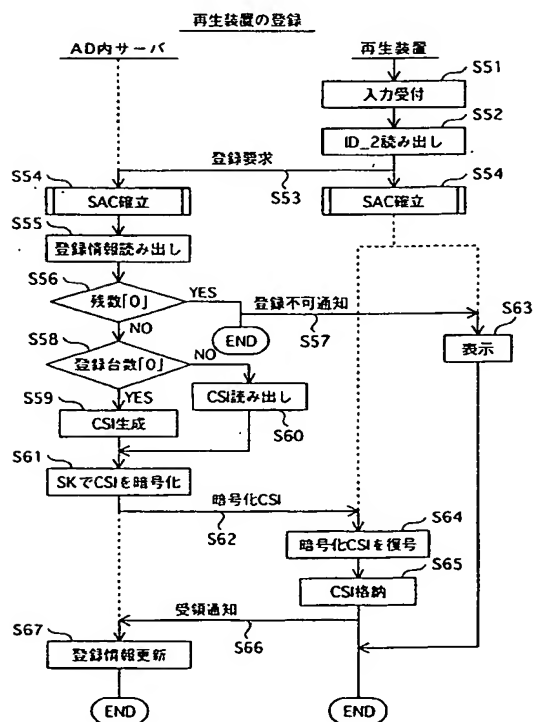
【図 6】



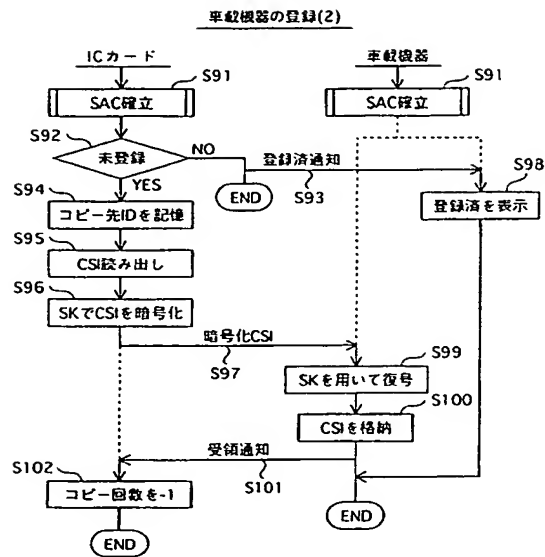
【 7 】



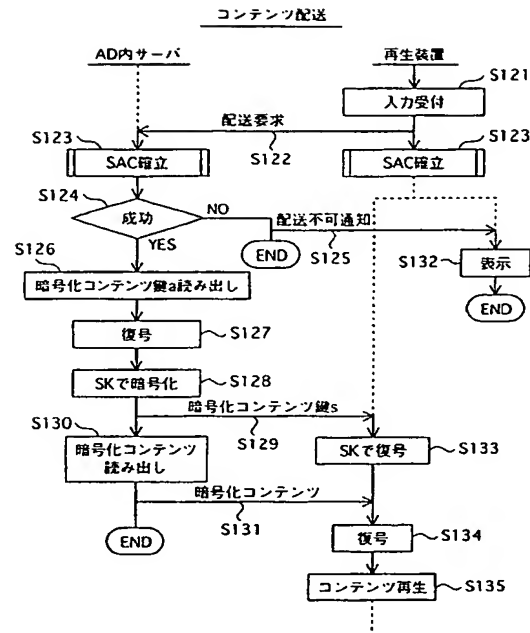
【 ㊦ 9 】



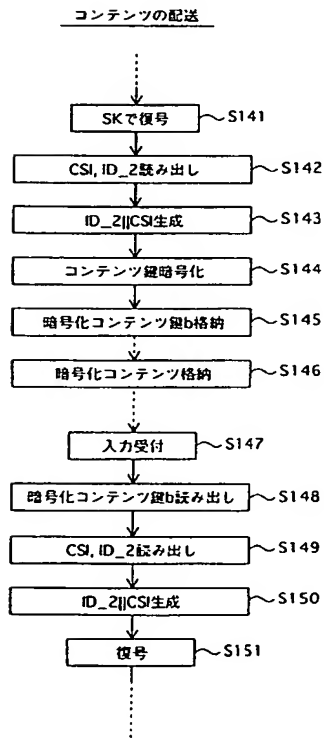
【図11】



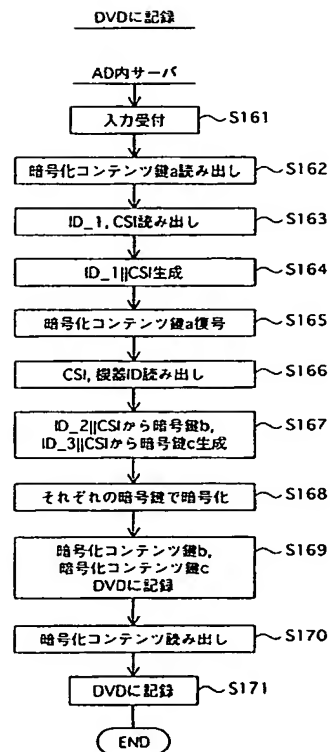
【図12】



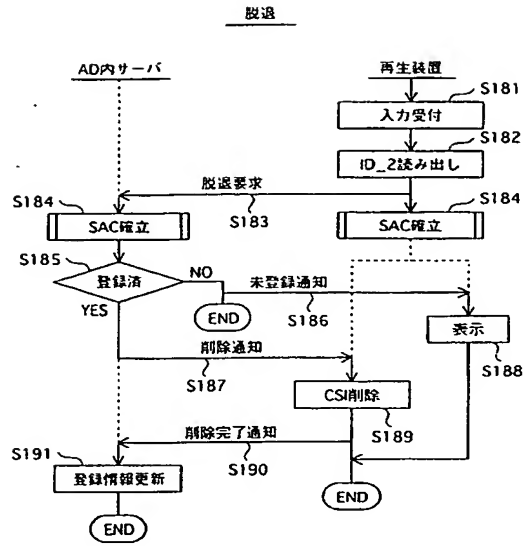
【図13】



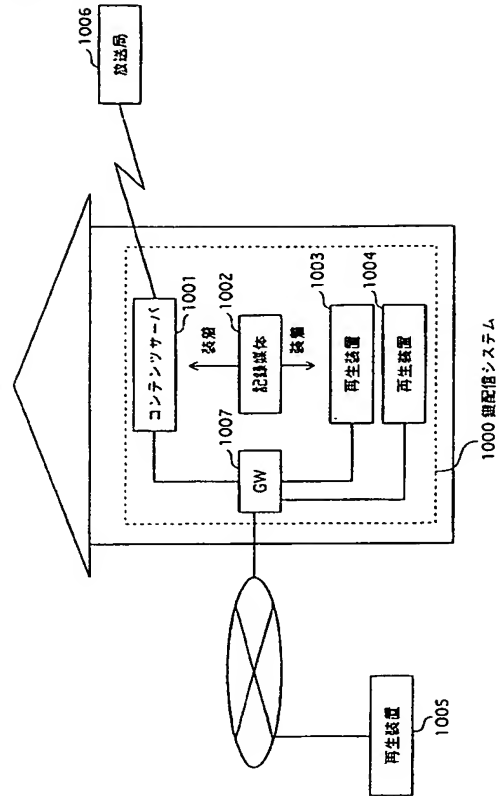
【図14】



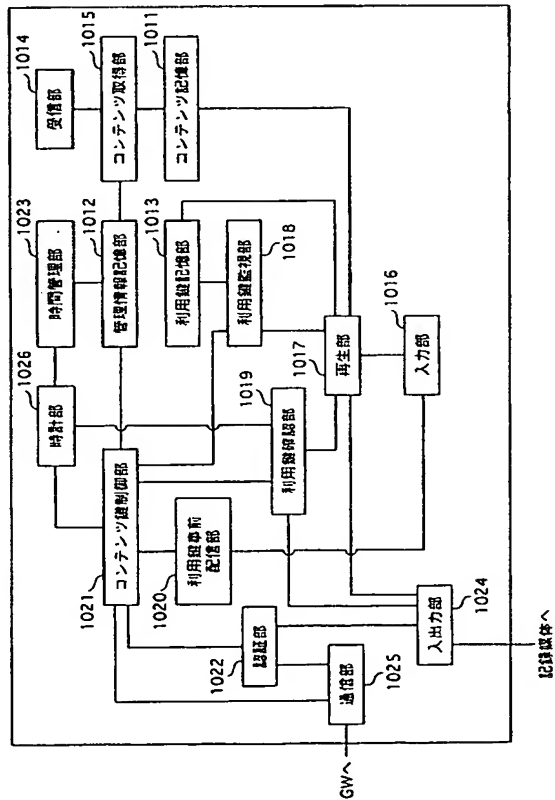
【図15】



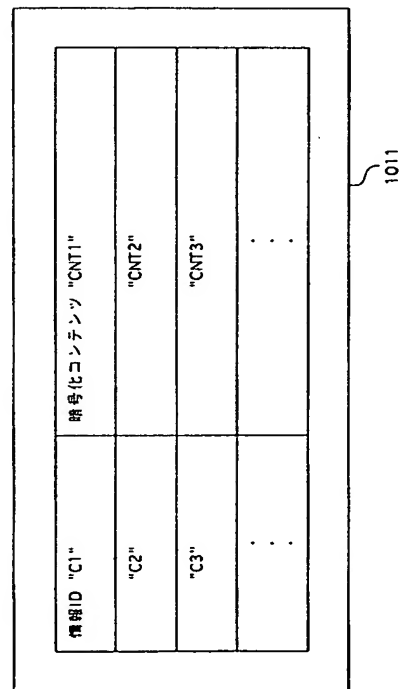
【図16】



【図17】

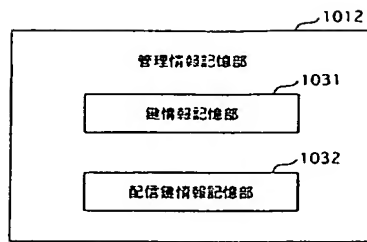


【図18】





【図 19】



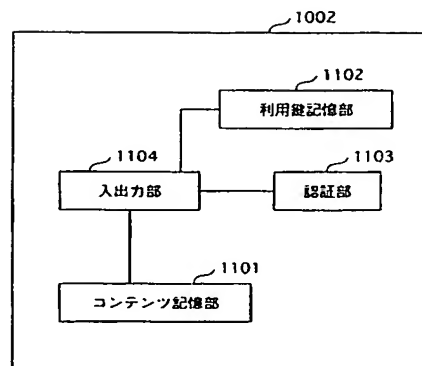
【図 20】

コンテンツID	コンテンツ種	対応情報ID	総数	種数	制限時間
1	CK1	C1	5	4	24時間
2	CK2	C2	5	3	24時間
3	CK3	C3	5	5	24時間
・	・	・	・	・	・

【図 21】

配信コンテンツID	利用期限
1	2003/7/10 19:00
2	2003/7/10 21:30
・	・
・	・

【図 22】

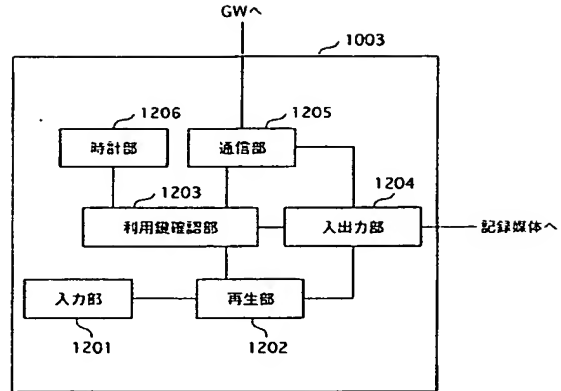


【図23】

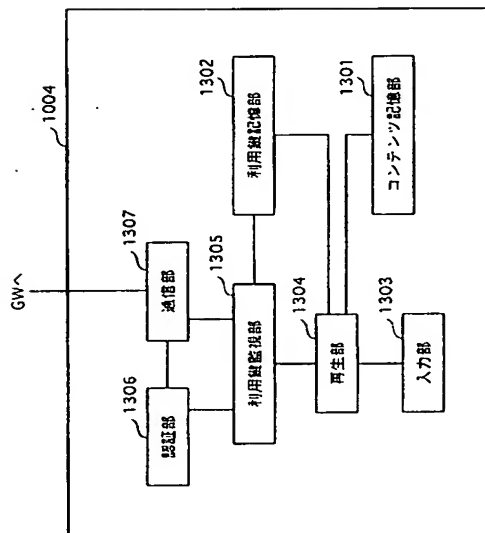
T1101

コンテンツID	コンテンツ値	対応情報ID	利用期限
1	CK1	C1	2003/7/10 19:00
2	CK2	C2	2003/7/10 21:30
...	...	...	...

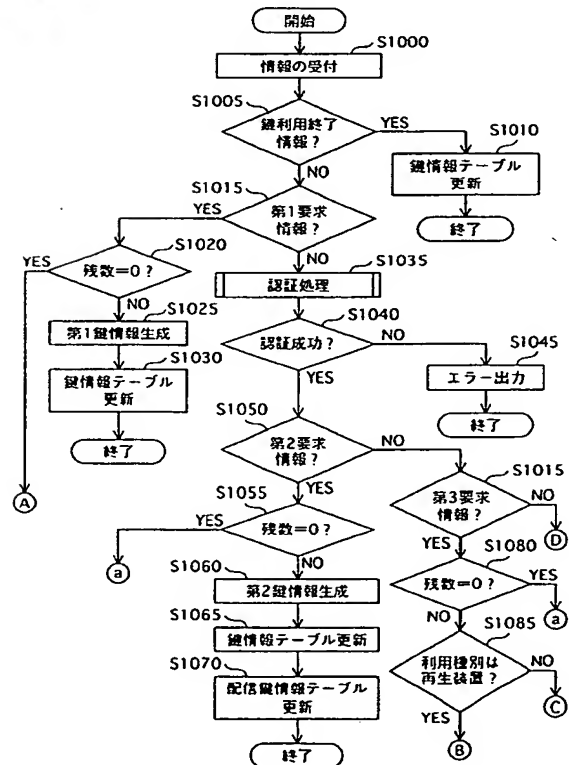
【図24】



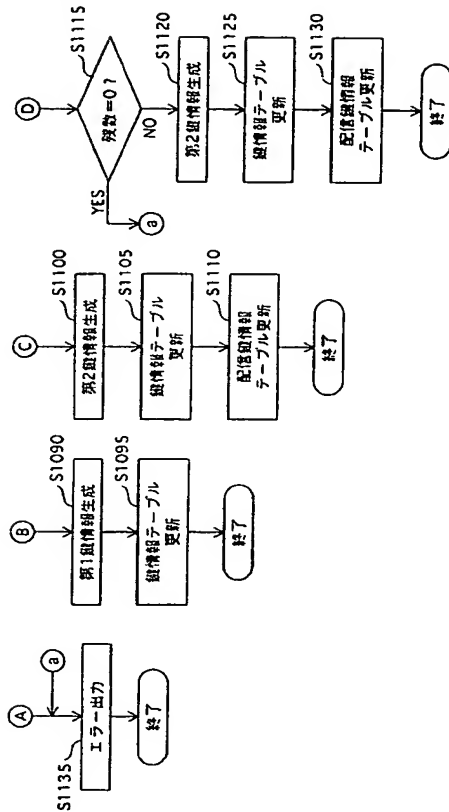
【図25】



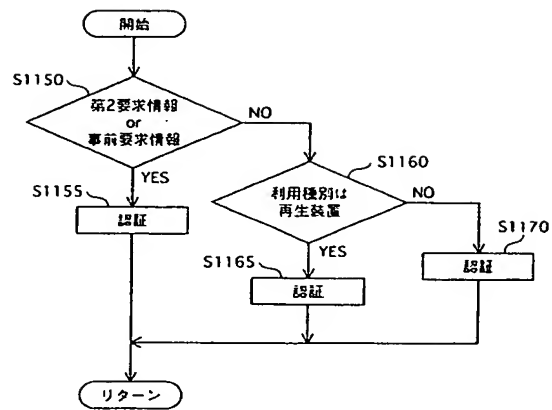
【図26】



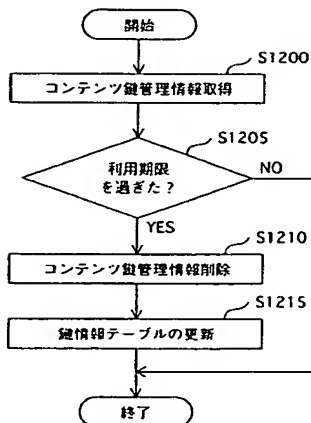
【図27】



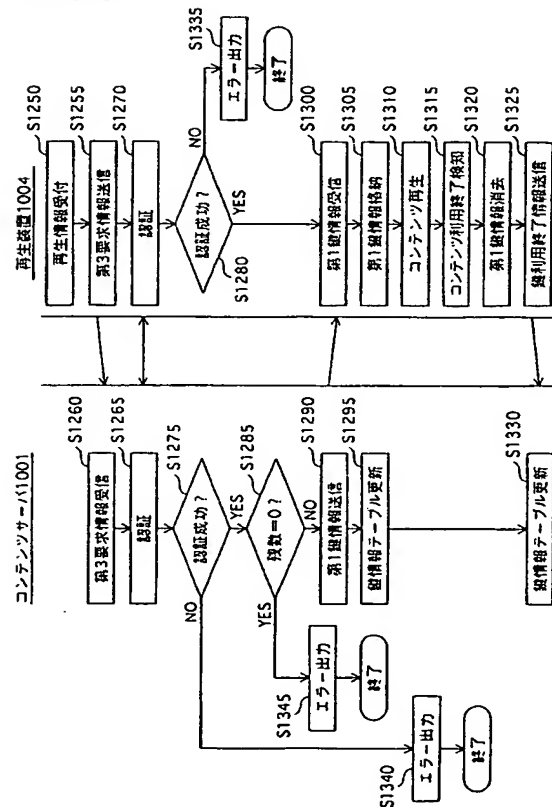
【図28】



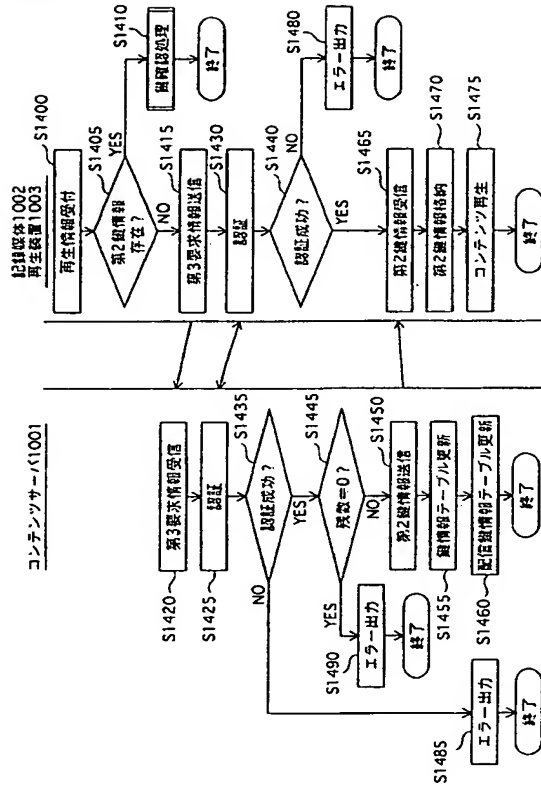
【図29】



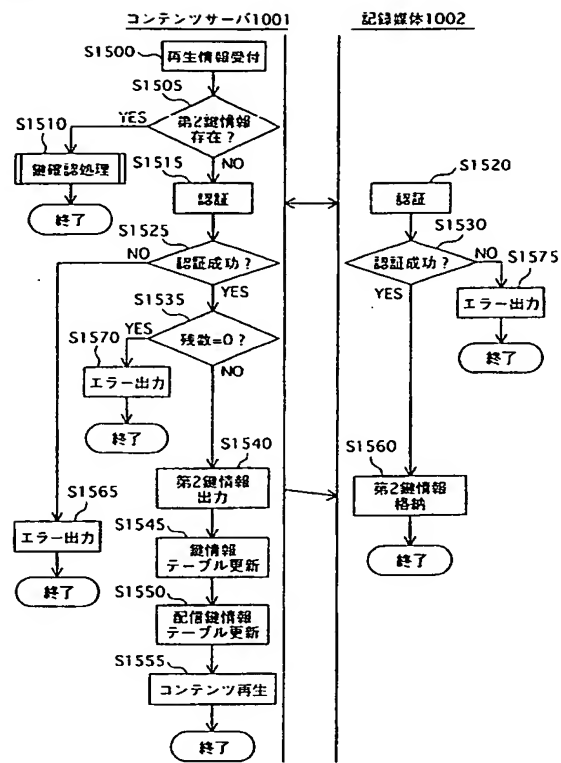
【図30】



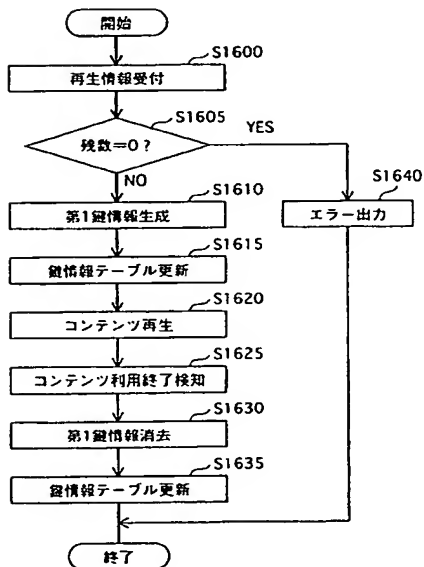
【図 3 1】



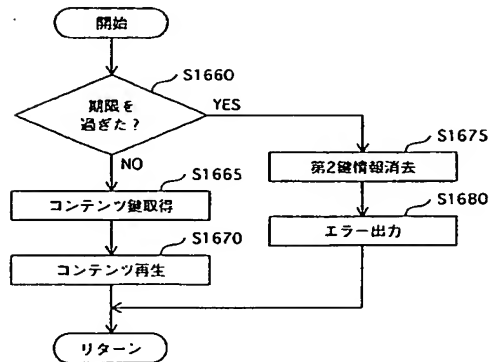
【図 3 2】



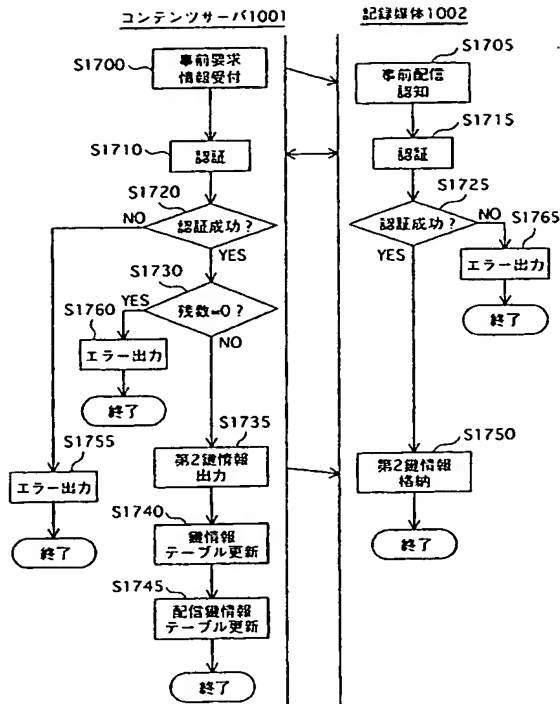
【図 3 3】



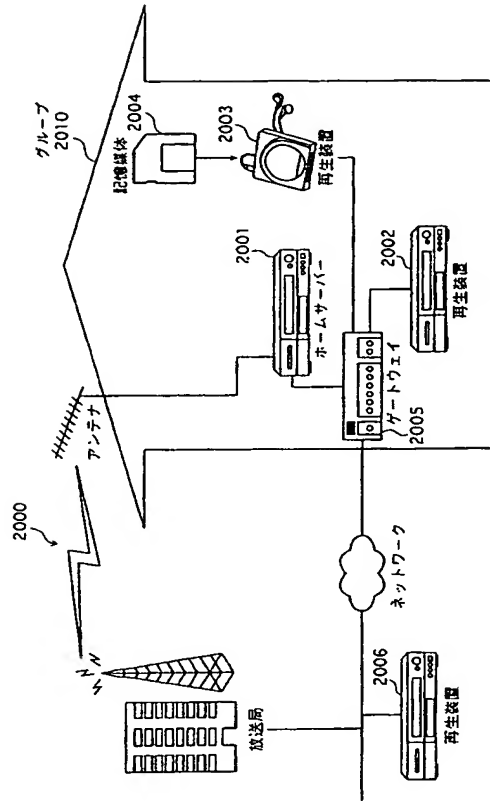
【図 3 4】



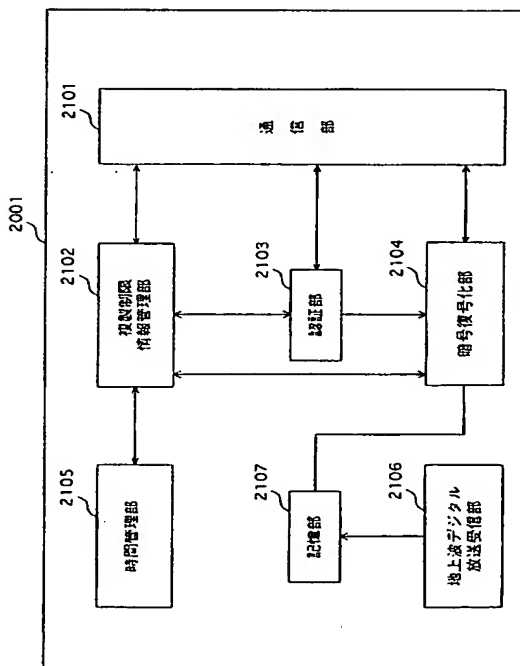
【図 35】



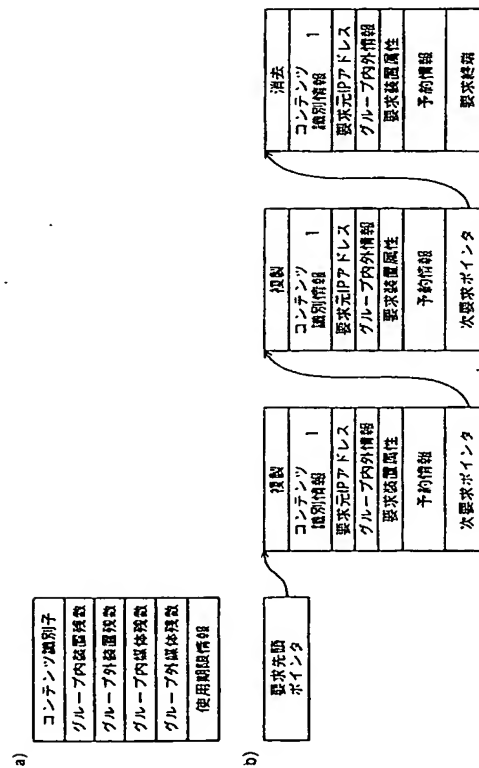
【図 36】



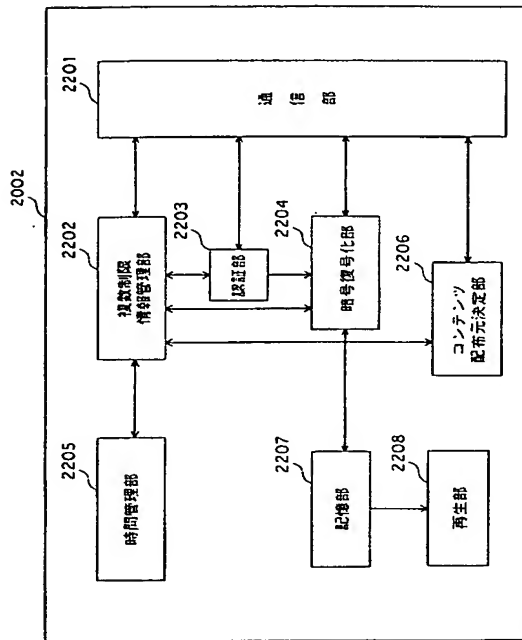
【図 37】



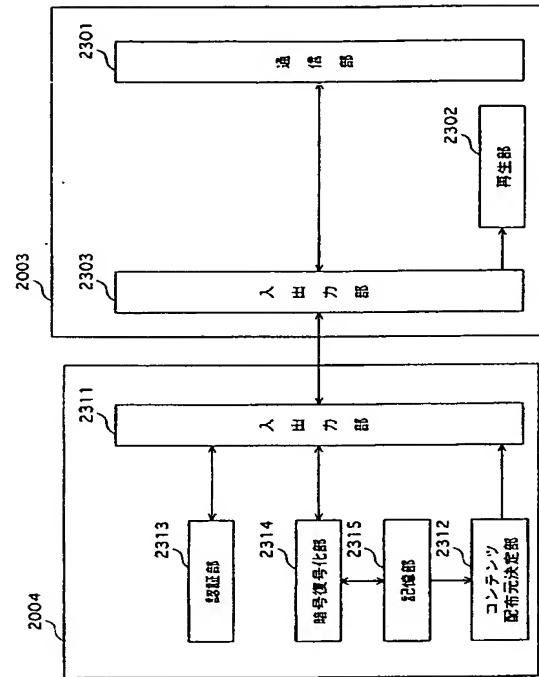
【図 38】



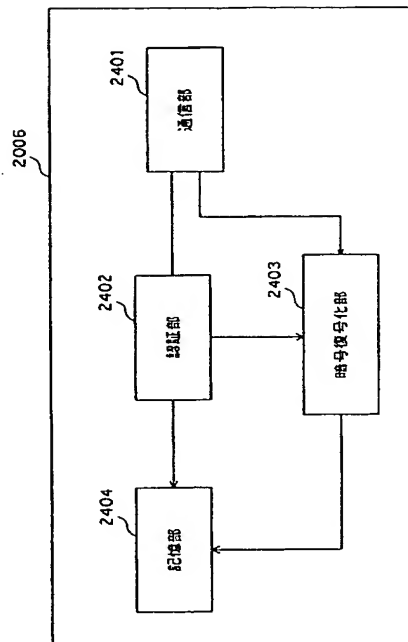
【図39】



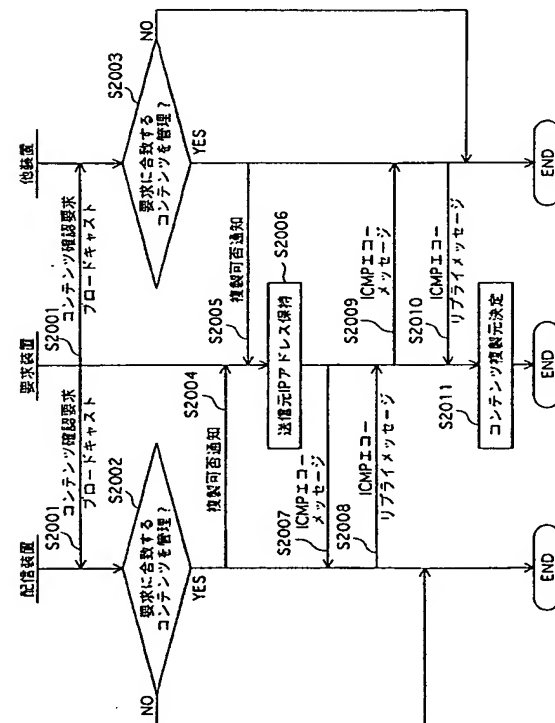
【図40】



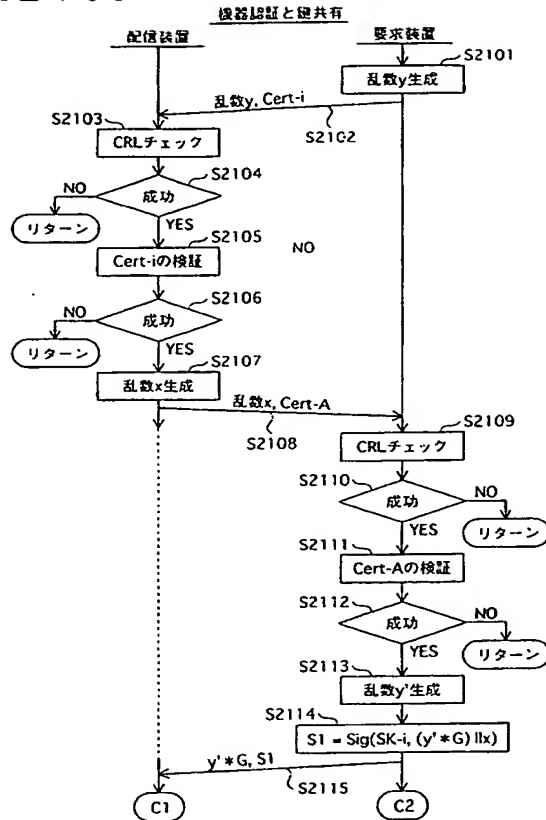
【図41】



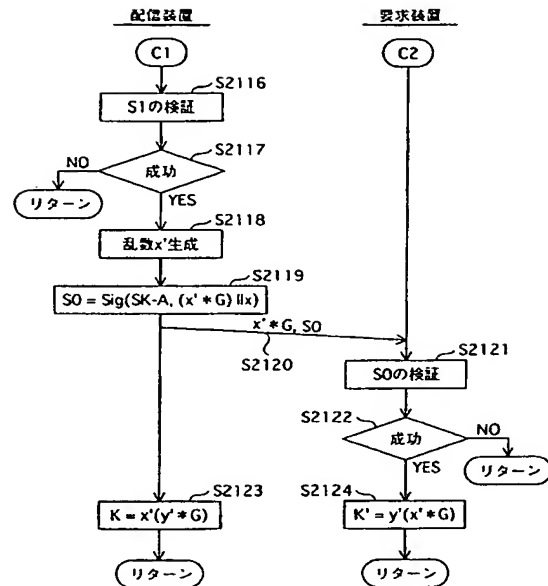
【図42】



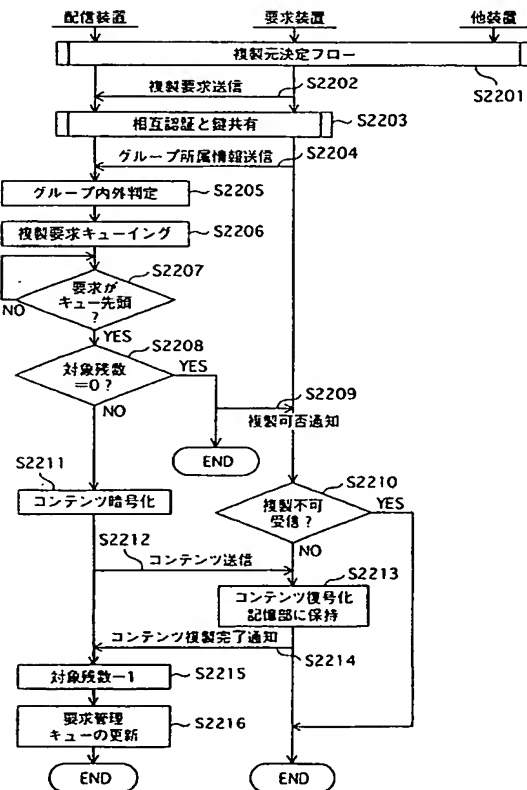
【図43】



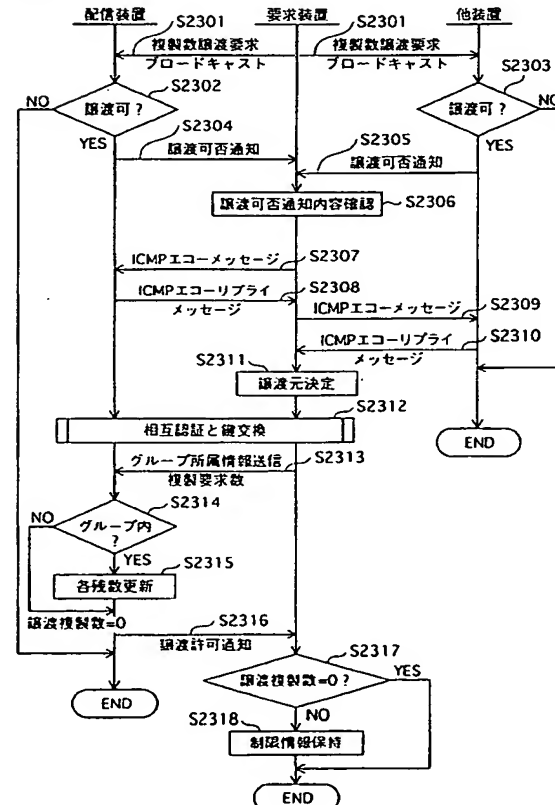
【図44】



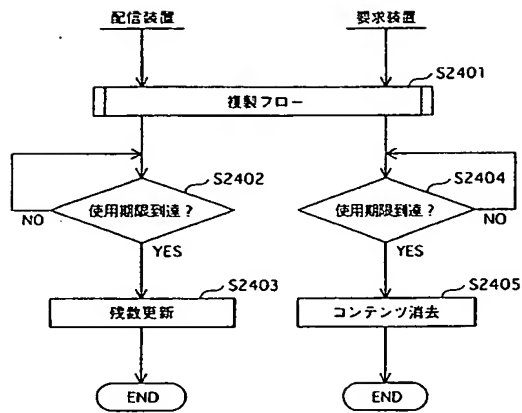
【図45】



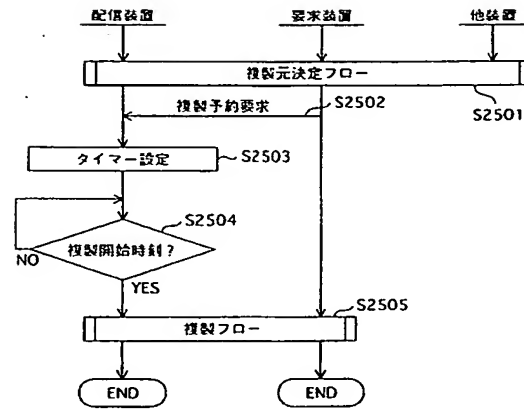
【図46】



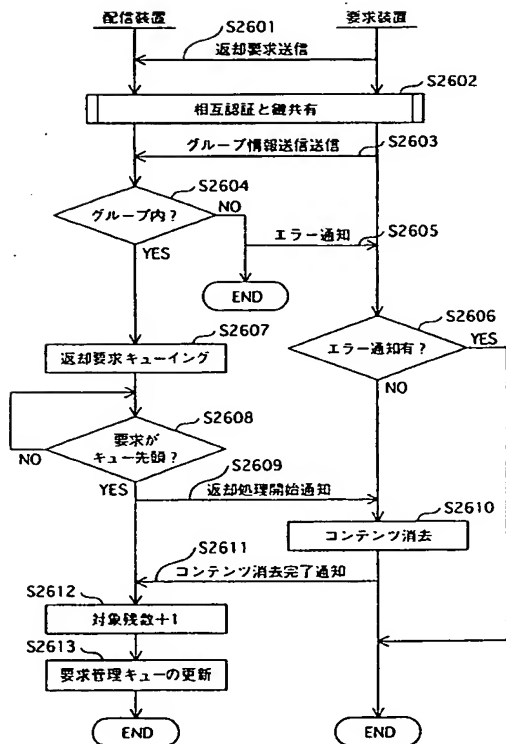
【図47】



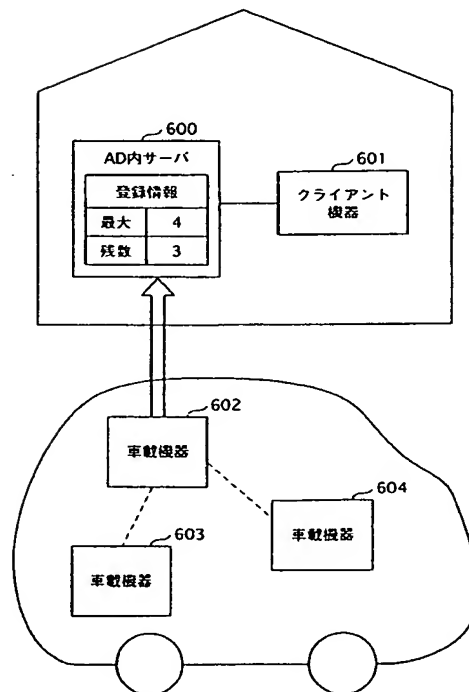
【図48】



【図49】

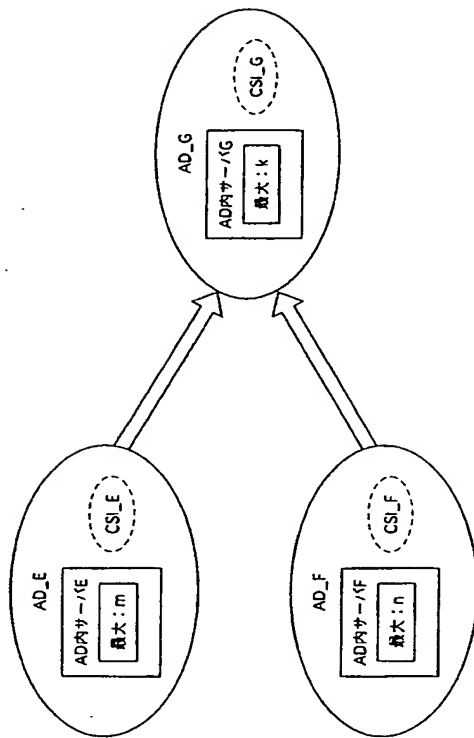


【図50】

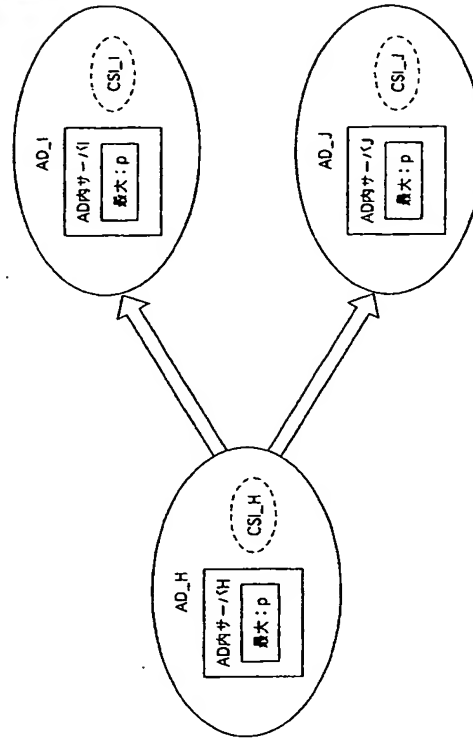




【図 5 1】



【図 5 2】



---

フロントページの続き

(72)発明者 松崎 なつめ

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72)発明者 阿部 敏久

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

Fターム(参考) 5J104 EA17

**This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**